ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU



SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

Security requirements for roadside unit in intelligent transportation systems

Recommendation ITU-T X.1379

T-UT



ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS X.1.199 OPEN SYSTEMS INTERCONNECTION X.200-X.299 INTERWORKING BETWEEN NETWORKS X.400-X.499 DRESAGE HADLING SYSTEMS X.600-X.699 OSI NETWORKING AND SYSTEM ASPECTS X.800-X.899 OSI NETWORKING AND SYSTEM ASPECTS X.800-X.899 OSI NETWORKING AND SYSTEM ASPECTS X.800-X.899 OSI APPLICATIONS X.800-X.819 OSI NETWORKING AND NETWORK SECURITY X.100-X.1029 General security aspects X.1000-X.1029 Network security anagement X.1000-X.1029 Security management X.1000-X.1029 Multicast security X.1110-X.1110 Home network security X.1110-X.1110 Multicast security X.110-X.1110		
OPEN SYSTEMS INTERCONNECTIONX.200-X.399INTERWORKING BETWEEN NETWORKSX.300-X.399MESSAGE HANDLING SYSTEM ASPECTSX.600-X.599OSI NETWORKING BETWEEN NETWORKSX.500-X.599OSI NETWORKING AND SYSTEM ASPECTSX.600-X.599OSI MANAGEMENTX.700-X.799SECURITYX.800-X.849OPEN DISTRIBUTED PROCESSINGX.800-X.849OPEN DISTRIBUTED PROCESSINGX.1000-X.1029Reneral security aspectsX.1000-X.1029NEVOKATION AND NETWORK SECURITYX.1000-X.1049General security managementX.1000-X.1049TelebiometricsX.1100-X.1109Home network securityX.1100-X.1109Home network securityX.1110-X.1119Web security (1)X.1140-X.1119Home network securityX.1120-X.1179Very Context of the securityX.1120-X.1179Very Context of the securityX.1120-X.1179Very Context of the securityX.1120-X.1179Very Context of the securityX.1120-X.1129Very Context of the securityX.1120-X.1129Very Context of the securityX.1200-X.1229Context of the securityX.130-X.1309Very Context of the secu	PUBLIC DATA NETWORKS	X.1–X.199
INTERWORKING BETWEEN NETWORKS X.400-X.499 DRESAGE HANDLING SYSTEMA SPECTS X.400-X.499 DRECTORY X.600-X.699 OSI METWORKING AND SYSTEM ASPECTS X.600-X.699 OSI MANAGEMENT X.200-X.799 ECURITY X.200-X.849 OSI APPLICATIONS X.200-X.849 DRECTING X.200-X.1029 Network security ASPECTS X.200-X.1029 Network security S.200-X.1030 Control X.200-X.1029 Network security S.200-X.1030 Control X.200-X.1029 Network security X.200-X.1030 Control X.200-X.1030 Control X.200-X.1030 Control X.200-X.1030 Control X.200-X.1040 Control X.200-X.204 CONTRUMICATION CONTRUENCENTY CONTRUENCENTY CONTRUENC	OPEN SYSTEMS INTERCONNECTION	X.200-X.299
MESSAGE HANDLING SYSTEMSX.400-X.499DIRECTORYX.500-X.599OSI NETWORKING AND SYSTEM ASPECTSX.600-X.599OSI MANAGEMENTX.700-X.799SEURITYX.800-X.849OPEN DISTRIBUTED PROCESSINGX.900-X.899OPEN DISTRIBUTED PROCESSINGX.1000-X.1029INFORMATION AND NETWORK SECURITYX.1000-X.1029General security aspectsX.1000-X.1029Network securityX.1000-X.1029SECURE APPLICATIONS AND SERVICES (1)X.1100-X.1109Hulticast securityX.1100-X.1109Security managementX.1100-X.1109Hubicast securityX.1110-X.1119Mobile security (1)X.1130-X.1139Hobs security (1)X.1140-X.1149Application Scourity (1)X.1150-X.1169Pert-o-peer securityX.1100-X.1179IPTV securityX.1300-X.1309SecurityX.130-X.130SecurityX.130-X.1310IPT SecurityX.130-X.1310IPT SecurityX.130-X.1319IPT SecurityX.130-X.1330IPT SecurityX.130-X.1330IPT Se	INTERWORKING BETWEEN NETWORKS	X.300-X.399
DIRECTORYX.500-X.599OSI NETWORKING AND SYSTEM ASPECTSX.600-X.699OSI METWORKING AND SYSTEM ASPECTSX.600-X.699OSI APPLICATIONSX.800-X.849OSI APPLICATIONSX.900-X.999INFORMATION AND NETWORK SECURITYX.1000-X.1029General security aspectsX.1000-X.1029Network security aspectsX.1000-X.1029Security managementX.1050-X.1049TelebiometricsX.1080-X.1099Security managementX.1000-X.1019Home network securityX.1100-X.1109Molite ascurityX.1100-X.1109Web security managementX.1100-X.1109Home network securityX.1100-X.1109Web security (1)X.1140-X.1139Home network securityX.1160-X.1169Per-to-peer Sourity (1)X.1160-X.1169Per-to-peer Sourity (1)X.1160-X.1169Per-to-peer Sourity (1)X.1160-X.1179Per-to-peer SourityX.1170-X.179Per-to-peer SourityX.1100-X.1129CyberscourityX.1230-X.1249Identity managementX.1230-X.1249Identity managementX.130-X.1309Discurity (2)X.1310-X.1319Security CommunicationsX.130-X.1309Ubiquitous sensor network securityX.130-X.1309Ubiquitous sensor network securityX.130-X.1309Ubiquitous sensor network securityX.130-X.1309Distributed ledger technology (DLT) securityX.130-X.1309Ubiquitous sensor network securityX.130-X.1309Distributed ledger technology (DLT) se	MESSAGE HANDLING SYSTEMS	X.400-X.499
ÖSI MANAGEMENTX.600-X.699OSI MANAGEMENTX.700-X.799SECURITYX.800-X.849OPEN DISTRIBUTED PROCESSINGX.850-X.899OPEN DISTRIBUTED PROCESSINGX.100-X.1029General security aspectsX.1000-X.1029Security managementX.1050-X.1049Security managementX.1050-X.1049Security managementX.1050-X.1049Security managementX.100-X.1129Hohme network securityX.110-X.1119Hohme network securityX.110-X.1139Web security (1)X.1140-X.1149Hohme network securityX.1140-X.1149Per-to-peer securityX.1140-X.1179PTV security (1)X.1160-X.1180Per-to-peer securityX.1120-X.1179PTV securityX.120-X.1229Cybersecurity curityX.120-X.1249Cybersecurity sensoreX.130-X.130CybersecurityX.130-X.1319Per-to-peer securityX.130-X.1249Cybersecurity sensore network securityX.130-X.1319Perto-peer securityX.130-X.1319Distributed ledger technology (DLT) securityX.130-X.139Security (2)X.1430-X.139Distributed ledger technology (DLT) securityX.130-X.139Distributed ledger technology (DLT) securityX.130-X.1489Cybersecurity (2)X.1400-X.1489Cybersecurity (2)X.1400-X.1489Cybersecurity (2)X.140-X.1489Cybersecurity (2)X.150-X.159Distributed ledger technology (DLT) securityX.130-X.159Distributed le	DIRECTORY	X.500-X.599
OSI MANAGEMENTX700-X799SOLUTYX800-X.849OSI APPLICATIONSX800-X.849OSI APPLICATIONSX800-X.849OSI APPLICATIONSX800-X.029INFORMATION AND NETWORK SECURITYX1000-X.1029General security spectsX1000-X.1029Security margementX100-X.1029Security securityX1100-X.1029Security securityX1100-X.1029Security securityX1100-X.1029Security securityX1100-X.1029Multicast securityX1100-X.1109Home network securityX1100-X.1119Hone network securityX1100-X.1109Hone network securityX1100-X.1119Hords securityX1160-X.1159Per-to-peer securityX1160-X.1159Per-to-peer securityX1160-X.1179Provented ID securityX1120-X.1129Per-to-peer securityX120-X.1249Identity managementX130-X.1309SeCURE APPLICATIONS AND SERVICES (2)X130-X.1319Emergency communicationsX130-X.1319Shart grd securityX130-X.1349Interfield unal transportation system (ITS) securityX130-X.1349Intelligent transportation system (ITS) securityX130-X.1349 </td <td>OSLNETWORKING AND SYSTEM ASPECTS</td> <td>X 600–X 699</td>	OSLNETWORKING AND SYSTEM ASPECTS	X 600–X 699
SECURITY X.800-X.849 OSI APPLICATIONS X.800-X.849 OSI APPLICATIONS X.800-X.899 INFORMATION AND NETWORK SECURITY General security aspects X.1000-X.1029 Network security X.1030-X.1049 Security management X.1030-X.1049 Telebiometrics X.1080-X.1060 Telebiometrics X.1080-X.1060 Telebiometrics X.1080-X.109 Home network security X.1100-X.1109 Home network security X.1100-X.1149 Peer-to-peer security X.1100-X.1149 Peer-to-peer security X.1100-X.1149 Peer-to-peer security X.1100-X.1149 Peer-to-peer security X.1100-X.1149 PirtV security X.1100-X.1150 V.1140-X.1150 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1140-X.130 V.1420 V.142	OSI MANAGEMENT	X 700-X 799
ONLAPPLICATIONSX.850-X.809OPEN DISTRIBUTED PROCESSINGX.850-X.809OPEN DISTRIBUTED PROCESSINGX.900-X.999INFORMATION AND NETWORK SECURITYX.1000-X.1029General security apactsX.1030-X.1049Security managementX.1050-X.1049Security managementX.1050-X.1049Multicast securityX.100-X.1109Borne network securityX.1100-X.1109Home network securityX.1100-X.1109Home network securityX.1100-X.1119Hobie Security (1)X.1150-X.1139Veb security (1)X.1150-X.1159Pert-o-peer securityX.1100-X.1179IPTV securityX.1100-X.1179IPTV securityX.1100-X.1179IPTV securityX.1100-X.1179IPTV securityX.1200-X.1229CybersecurityX.1200-X.1249CybersecurityX.130-X.139Councting spanX.1200-X.1249Identity managementX.130-X.139SecURE APPLICATIONS AND SERVICES (2)X.130-X.139Emergency communicationsX.130-X.139Using utel deger technology (DLT) securityX.1400-X.1490Ubiguitous sensor network securityX.130-X.139Internet of things (IGT) securityX.1400-X.1429Application Security (2)X.1470-X.139Using utel deger technology (DLT) securityX.1400-X.1429Application Security (2)X.1400-X.1429Cybersecurity (2)X.1400-X.1429Cybersecurity (2)X.1400-X.1459Cyber DefenceX.1500-X.1599Cloud Computi	SECURITY	X 800-X 849
OBEN DISTRIBUTED PROCESSINGX.300-X.399INFORMATION AND NETWORK SECURITYX.900-X.1029Qeneral security aspectsX.1000-X.1029Network securityX.1030-X.1049Security managementX.1050-X.1060TelebiometricsX.1000-X.1029SECURE APPLICATIONS AND SERVICES (1)X.1100-X.1109Home network securityX.1100-X.1109Home network securityX.1100-X.1119Multicast securityX.1100-X.1120Home network securityX.1100-X.1149Peter-to-peer securityX.1100-X.1149Peter-to-peer securityX.1100-X.1169Peter-to-peer securityX.1120-X.1179Problem securityX.1120-X.1179CYBERSPACE SECURITYX.1200-X.1229Countering spamX.1200-X.1229Countering spamX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.130-X.1309Ubigitent transportation system (TS) securityX.1400-X.1429Application Security (2)X.1470-X.1489CYBERSECURITY (NFORMATION EXCHANGEX.1500-X.1519Overview of cybensecurityX.1500-X.1519Vuerability/site sechangeX.1500-X.1519Vuerability/site sechangeX.1500-X.1519Vuerability/site sechangeX.1500-X.1519CUDD COMPUTING SECURITYX.1600-X.1601Cload computing se		X.800 - X.849 X.850 - X.800
Delevide the processing and a security aspects (Control of the processing and a security and agence (Control of the processing and a security and agence (Control of the processing and a security and agence (Control of the processing and a security (Control of the processing and		X.030 - X.033
INFORMATION AND NETWORK SECURITY General security anagement X.1030-X.1029 Network security X.1030-X.1049 Security management X.1050-X.1069 Telebiometrics X.1080-X.109 Telebiometrics X.1080-X.109 SECURE APPLICATIONS AND SERVICES (1) Multicast security X.1100-X.1119 Mobile security X.1100-X.1119 Mobile security (1) X.1140-X.1149 Application Security (1) Y.1140-X.1149 Peer-to-per security X.1160-X.1159 Peer-to-per security X.1160-X.1169 Y.1170-X.1179 UPV security X.1160-X.1169 Y.1170-X.1179 UPV security X.1160-X.1169 Y.1170-X.1179 Y.1170-X.1179 UPV security X.1200-X.1229 Countering span X.1230-X.1249 Identity management X.1300-X.1309 Ubiquitous sensor network security X.1300-X.1309 Ubiquitous sensor network security X.1300-X.1309 Distributed ledger technology (DLT) security X.1300-X.1309 Distributed ledger technology (DLT) security X.1300-X.1309 Distributed ledger technology (DLT) security X.1300-X.1399 Distributed ledger technology (DLT) security X.1300-X.1399 Distributed ledger technology (DLT) security X.1400-X.1429 Application security (2) X.1470-X.1489 CYBERSECURITY NFORMATION EXCHANGE Overview of cloud computing security X.1500-X.159 Heuristics exchange X.1500-X.159 Heuristics exchange X.1500-X.159 Heuristics exchange X.1500-X.159 Cloud computing security X.1500-X.169 Cloud computing security X.150-X	UNEODMATIONI AND NETWORK SECURITY	A.900–A.999
Centeral security anagementX.1000-X.1029Security managementX.1050-X.1069TelebiometricsX.1060-X.1099SECURE APPLICATIONS AND SERVICES (1)X.1100-X.1109Multicast securityX.1100-X.1109Home network securityX.1100-X.1109Mobile security (1)X.1140-X.1119Application Security (1)X.1150-X.1159Peer-to-peer securityX.1160-X.1179IPTV securityX.1160-X.1179IPTV securityX.1120-X.1139CybersecurityX.1120-X.1139CybersecurityX.1120-X.1179IPTV securityX.1120-X.1129Contering spamX.1200-X.1229Countering spamX.1200-X.1229Countering spamX.1200-X.1229Countering spamX.130-X.1339Ubiquitous sensor network securityX.130-X.1339Distributed ledger technology (DLT) securityX.130-X.1339Intelligent transportation system (ITS) securityX.130-X.1339Distributed ledger technology (DLT) securityX.140-X.1429Application security (2)X.140-X.1439CybersecurityX.150-X.1599Vulnerability'state exchangeX.150-X.159Vulnerability'state exchangeX.150-X.159Pourity of cybersecurityX.150-X.159Heuristics and information requestX.150-X.159Heuristics and information requestX.150-X.159Heuristics and information requestX.150-X.159Heuristics and information requestX.150-X.159Identification and discoveryX.150-X.159 <td< td=""><td>INFORMATION AND NETWORK SECORITY</td><td>X 1000 X 1020</td></td<>	INFORMATION AND NETWORK SECORITY	X 1000 X 1020
Network securityX.1030–X.1049Security managementX.1050–X.1069TelebiometricsX.1080–X.1099SECURE APPLICATIONS AND SERVICES (1)X.1100–X.1109Multicast securityX.1100–X.1109Home network securityX.1100–X.1139Web security (1)X.1140–X.1144Application Security (1)X.1140–X.1149Peer-to-peer securityX.1160–X.1160Networked ID securityX.1160–X.1179IPTV securityX.1100–X.1179IPTV securityX.1200–X.1229Councering spanX.1230–X.1249Identity managementX.1300–X.1309Ubiquitous sensor network securityX.130–X.1319SecURE APPLICATIONS AND SERVICES (2)X.1300–X.1339Emergency communicationsX.1300–X.1339Ubiquitous sensor network securityX.130–X.1319Distributed ledger technology (DLT) securityX.130–X.1339Distributed ledger technology (DLT) securityX.1400–X.1429Application Security (2)X.1470–X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500–X.1519Overview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Councering security designX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Vulnerability/state exchangeX.1500–X.1519Overview of cybersecurityX.1500–X.1519Overview	General security aspects	X.1000–X.1029
Security managementX.1050–X.1099SECURE APPLICATIONS AND SERVICES (1)X.000–X.1009Multicast securityX.1100–X.1109Home network securityX.1100–X.1110Mobile security (1)X.1140–X.1139Year-to-peer security (1)X.1150–X.1159Peer-to-peer security (1)X.1160–X.1169Peer-to-peer securityX.1160–X.1179IPTV securityX.1100–X.1179IPTV securityX.1200–X.1229Countering spamX.1200–X.1229Countering spamX.1200–X.1229Countering spamX.1200–X.1229Identity managementX.1200–X.1229SECURE APPLICATIONS AND SERVICES (2)X.1300–X.1309Emergency communicationsX.1300–X.1309Ubiquitous sensor network securityX.1300–X.1309Ubiquitous sensor network securityX.1300–X.1309Intelligent transportation system (ITS) securityX.1300–X.1309Intelligent transportation system (ITS) securityX.1400–X.1429Application Security (2)X.1400–X.1429Valproise control of security (2)X.1400–X.1439Overview of cybersecurityX.1500–X.159Vulnerability'state exchangeX.1500–X.159Heuristics and information requestX.1500–X.159Heuristics and information requestX.1500–X.159Identity managementX.1500–X.159Overview of cloud computing securityX.160–X.169Overview of cloud computing securityX.1500–X.159Heuristics and information requestX.1500–X.159Identity managementX.1500–X.15	Network security	X.1030–X.1049
Telebiometrics X.1080–X.1099 SECURE APPLICATIONS AND SERVICES (1) Multicast security X.1100–X.1109 Home network security X.1100–X.1109 Mobile socurity X.1100–X.1109 Mobile socurity X.1100–X.1109 Mobile socurity X.1100–X.1139 Web security (1) X.1150–X.1139 Per-to-per security X.1100–X.1170 Per-to-per security X.1100–X.1170 V.1170–X.1179 PTV security X.1100–X.1179 PTV security X.1100–X.1179 PTV security X.1200–X.129 Countering span X.1230–X.1249 Identity management X.1210–X.129 SECURE APPLICATIONS AND SERVICES (2) Emergency communications X.1310–X.1309 Ubiquitous sensor network security X.130–X.1309 Ubiquitous sensor network security X.130–X.1400 V.1400–X.1400–X.1429 Polication Security X.130–X.1409 Ubication for security X.130–X.1429 Polication Security X.1400–X.1429 Polication Security X.1400–X.1429 CYBERSECURITY INFORMATION EXCHANGE UPVerview of cybersecurity X.150–X.1509 Evchange of policies X.150–X.1599 Evchange of policies X.150–X.1599 CLOUD COMPUTING SECURITY UPVerview of Cloud computing security X.150–X.1509 CLOUD COMPUTING SECURITY UPVerview of Cloud compu	Security management	X.1050–X.1069
SECURE APPLICATIONS AND SERVICES (1) Huticast security X.1100-X.1109 Home network security X.1100-X.1109 X.1100-X.1139 Web security (1) Application Security (1) Application Security (1) Peer-to-peer security X.1160-X.1169 Networked ID security X.1170-X.1179 PTV security X.1170-X.1179 CYBERSPACE SECURITY Cybersceurity X.1200-X.129 Countering spam X.1200-X.129 SECURE APPLICATIONS AND SERVICES (2) Emergency communications X.1300-X.1309 Distributed ledger technology (DLT) security N.1300-X.1399 Distributed ledger technology (DLT) security Vulnerability/state exchange CYBERSECURITY NIFORMATION EXCHANGE CYDERSECURITY NIFORMATION EXCHANGE CYBERSECURITY NIFORMATION EXCHANGE CYBERSECURITY NIFORMATION EXCHANGE CYDERSECURITY N	Telebiometrics	X.1080–X.1099
Multicast securityX.1100-X.1109Home network securityX.1110-X.1119Mobile security (1)X.1120-X.1139Application Security (1)X.1150-X.1159Pert-to-per securityX.1160-X.1169Networked ID securityX.1170-X.1179IPTV securityX.1170-X.1179CYBERSPACE SECURITYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.130-X.139SECURE APPLICATIONS AND SERVICES (2)X.130-X.139Emergency communicationsX.130-X.139Ubiquitous sensor network securityX.130-X.139Jost of things (GT) securityX.130-X.139Internet of things (GT) securityX.130-X.139Internet of things (GT) securityX.130-X.139VeryBERSECURITY INFORMATION EXCHANGEX.1400-X.1489CYBERSECURITY INFORMATION EXCHANGEX.1600-X.1489CyBERSECURITY INFORMATION EXCHANGEX.1500-X.159Vulnerability/state exchangeX.150-X.159Exchange of policiesX.150-X.159Exchange of policiesX.150-X.159Cyber befenceX.1500-X.159Cuontring accurity designX.1600-X.159Cuontring security designX.1600-X.160Cyber befenceX.1500-X.159Cuontring accurity designX.1600-X.159Cuontring accurity designX.1600-X.159Cuontring accurity designX.1600-X.159Cuontring accurity designX.160-X.169Cuontring accurity designX.160-X.169Cuontring accurity designX.160-X.169Cuontring a	SECURE APPLICATIONS AND SERVICES (1)	
Home network securityX.110–X.1119Mobile security (1)X.1140–X.1149Application Security (1)X.1140–X.1149Application Security (1)X.1160–X.1159Peer-to-peer securityX.1160–X.1169Networked ID securityX.1170–X.1179PTV securityX.1180–X.1180CYBERSPACE SECURITYX.1200–X.1229Countering spanX.1200–X.1279Identity managementX.130–X.1249Ubiquitous sensor network securityX.130–X.1309Ubiquitous sensor network securityX.130–X.1349Identity managementX.130–X.1349SecurityX.130–X.1349Ubiquitous sensor network securityX.130–X.1349Intelligent transportation system (ITS) securityX.1370–X.1399Distributed ledger technology (DLT) securityX.1450–X.1459Vulnerability/state exchangeX.150–X.1519Vulnerability/state exchangeX.150–X.1599Vulnerability/state exchangeX.150–X.1599Vulnerability/state exchangeX.150–X.1599Cyber DefenceX.150–X.1599Cloud computing security designX.160–X.1601Cloud computing security best practices and guidelinesX.160–X.1699Cloud computing security best practices and guidelinesX.160–X.1609Cloud computing security best practices and guidelinesX.160–X.1619Cloud computing security best practices and guidelinesX.160–X.1619Cloud computing security best practices and guidelinesX.160–X.1619Cloud computing security best practices and guidelinesX.160–X.1619<	Multicast security	X.1100–X.1109
Mobile securityX.1120-X.1139Web security (1)X.1140-X.1149Application Security (1)X.1150-X.1159Peer-to-peer securityX.1160-X.1179PITV securityX.1170-X.1179IPTV securityX.1170-X.1179IPTV securityX.1170-X.1179IPTV securityX.1200-X.129Countering spamX.1230-X.1249Identity managementX.1230-X.1249Identity managementX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Ubiquitous sensor network securityX.1300-X.1309Internet of things (IoT) securityX.1300-X.1399Internet of things (IoT) securityX.1300-X.1399Distributed ledger technology (DLT) securityX.1400-X.1429Veb security (2)X.1470-X.1439Vulnerability/state exchangeX.1500-X.159Overview of cybersecurityX.1500-X.159Vulnerability/state exchangeX.1500-X.159Heuristics and information requestX.1500-X.159Identification and discoveryX.150-X.159Cloud computing security best practices and guidelinesX.1600-X.1601Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619C	Home network security	X.1110–X.1119
Web security (1)X.1140-X.1149Application Security (1)X.1150-X.1159Peer-to-peer securityX.1160-X.1169Networked ID securityX.1170-X.1179PTV securityX.1180-X.1199CYBERSPACE SECURITYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1230-X.1249SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Emergency communicationsX.1300-X.1309Smart grid securityX.1310-X.1319Smart grid securityX.1330-X.1349Internet of things (617) securityX.1340-X.1349Internet of things (617) securityX.1370-X.1399Distributed ledger technology (DLT) securityX.1400-X.1429Application Security (2)X.1470-X.1459CYBERSECURITY INFORMATION EXCHANGEX.1500-X.1519Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Event/incident/heuristics exchangeX.1500-X.1519Event/incident/heuristics exchangeX.1500-X.1519Event/incident/heuristics exchangeX.1500-X.1519CLOUD COMPUTING SECURITYX.1500-X.1519Overview of cloud computing securityX.1600-X.1611Cloud computing security best practices and guidelinesX.1600-X.1611Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1611Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1	Mobile security	X.1120-X.1139
Application Security (1)X.1150-X.1159Peer-to-peer securityX.1160-X.1169Networked ID securityX.1170-X.1179IPTV securityX.1170-X.1179IPTV securityX.1170-X.1179CYBERSPACE SECURTYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1200-X.1249Identity managementX.130-X.1309SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.1310-X.1339Ubiquitous sensor network securityX.1340-X.1349Smart grid securityX.1340-X.1349Uhingent transportation system (ITS) securityX.1340-X.1349Intelligent transportation system (ITS) securityX.1400-X.1459Vulnerability/state exchangeX.1500-X.1519Vulnerability/state exchangeX.1500-X.1539Vulnerability/state exchangeX.1500-X.1549Vulnerability/state exchangeX.1500-X.1549Vulnerability/state exchangeX.1500-X.1549Vulnerability/state exchangeX.1500-X.1549Vulnerability/state exchangeX.1500-X.1549CUOUD COMPUTING SECURITYX.1600-X.1659CLOUD COMPUTING SECURITYX.1600-X.1659Cloud computing security best practices and guidelinesX.1600-X.1659Cloud computing security best practices and guidelinesX.1602-X.1639Cloud computing security best practices and guidelinesX.1602-X.1639Cloud computing security best practices and guidelinesX.1602-X.1639Cloud computi	Web security (1)	X.1140–X.1149
Peer-to-peer securityX.1160-X.1169Networked ID securityX.1170-X.1179IPTV securityX.1180-X.1199CYBERSPACE SECURITYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.130-X.1339Certified mailX.130-X.1339Interligent transportation system (ITS) securityX.130-X.1339Intelligent transportation system (ITS) securityX.130-X.1339Overview of cybersecurityX.130-X.1349Vulnerability/state sechangeX.1450-X.1459Web security (2)X.1450-X.1459Vulnerability/state sechangeX.1500-X.1519Vulnerability/state sechangeX.1500-X.1519Overview of cybersecurityX.1500-X.1519Vulnerability/state sechangeX.1500-X.1519Exchange of policiesX.1500-X.1519Vulnerability/state sechangeX.1500-X.1519Vulnerability/state sechangeX.1500-X.1519COUD COMPUTING SECURITYX.1500-X.1559Identification and discoveryX.1500-X.1559Identification and discoveryX.1600-X.1639Cloud computing security bestratices and guidelinesX.1600-X.1619Overview of cloud computing securityX.1600-X.1639Cloud computing security bestratices and guidelinesX.1600-X.1639Cloud computing security bestratices and guidelinesX.1600-X.1639Cloud computing security bestratices and guidelinesX.1600-X.1639Cloud computing security bestra	Application Security (1)	X.1150-X.1159
Networked ID securityX.1170-X.1179IPTV securityX.1180-X.1199CYBERSPCE SECURITYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1230-X.1249Identity managementX.1230-X.1249SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1319Emergency communicationsX.1300-X.1339Smart grid securityX.1310-X.1349Smart grid securityX.1300-X.1339Distributed ledger technology (DLT) securityX.1370-X.1399Distributed ledger technology (DLT) securityX.1470-X.1429Application Security (2)X.1470-X.1439Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Vulnerability/state exchangeX.1500-X.1559Event/incident/heuristics exchangeX.1500-X.1559Heuristics and information requestX.1500-X.1599CLOUD COMPUTING SECURITYX.1600-X.1601Cloud computing securityX.1600-X.1619Overview of cloud computing securityX.1600-X.1619Overview of oldu computing securityX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619Outerview of cloud computing securityX.1600-X.1619Outerview of cloud computing securityX.1600-X.1619Outerview of cloud computing securityX.1600-X.1719Framework of QKDN security designX.1700-X.1799Framewo	Peer-to-peer security	X.1160-X.1169
IntroductionIntroductionIPTV securityX.1180-X.1199CYBERSPACE SECURITYX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1230-X.1249SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Emergency communicationsX.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.1330-X.1339Certified mailX.1330-X.1339Internet of things (IoT) securityX.1330-X.1339Distributed ledger technology (DLT) securityX.1400-X.1429Application Security (2)X.1470-X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500-X.1519Overview of cybersecurity (2)X.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Vulnerability/state exchangeX.1500-X.1559Heuristics and information requestX.1500-X.1559Heuristics and information requestX.1500-X.1599CLOUD COMPUTING SECURITYX.1600-X.1610Cloud computing security orX.1600-X.1619Overview of cloud computing securityX.1600-X.1619Outer of cloud computing securityX.1600-X.1619Outer of cloud computing securityX.1600-X.1619Out of cloud computing securityX.1600-X.1619 <td< td=""><td>Networked ID security</td><td>X 1170-X 1179</td></td<>	Networked ID security	X 1170-X 1179
CYBERSPACESECURITYCYBERSPACEX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1230-X.1249SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Emergency communicationsX.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.130-X.1339Certified mailX.130-X.1339Intelligent transportation system (ITS) securityX.130-X.1349Distributed ledger technology (DLT) securityX.1400-X.1439Poligent transportation system (ITS) securityX.1400-X.1439Verbrew of cybersecurity (2)X.1470-X.1489CYBERSECURITY INFORMATION EXCHANGEV.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1519Vuherability/state exchangeX.1500-X.1559Heuristics and information requestX.1500-X.1559Identification and discoveryX.1500-X.159CLOUD COMPUTING SECURITYVerview of cloud computing securityOverview of cloud computing security best practices and guidelinesX.1600-X.1639Cloud computing security best practices and guidelinesX.1600-X.1639Cloud computing security best practices and guidelinesX.160	IPTV security	X 1180-X 1199
CybersecurityX.1200-X.1229Countering spamX.1230-X.1249Identity managementX.1230-X.1249SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Emergency communicationsX.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.130-X.1339Certified mailX.1350-X.1339Internet of things (IoT) securityX.1340-X.1349Interligent transportation system (ITS) securityX.1470-X.1429Application Security (2)X.1470-X.1429Vulnerability/state exchangeX.1500-X.1519Overview of cybersecurityX.1470-X.1489Vulnerability/state exchangeX.1500-X.1519Pleuristics and information requestX.1500-X.1519Identification and discoveryX.1570-X.1579Assured exchangeX.1570-X.1579CUDD COMPUTING SECURITYX.1600-X.1601Cloud computing security designX.1600-X.1601Cloud computing security designX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security designX.1600-X.1619Cloud computing security designX.170	CYBERSPACE SECURITY	M .1100 M .1199
Countering spam Countering spam Lizon-X.1249 Mentity management SECURE APPLICATIONS AND SERVICES (2) Emergency communications Ubiquitous sensor network security Smart grid security X.1310-X.1309 Ubiquitous sensor network security Smart grid security X.1310-X.1319 X.1310-X.1339 Certified mail X.130-X.1339 Intelligent transportation system (ITS) security X.1370-X.1399 Distributed ledger technology (DLT) security X.1370-X.1399 Distributed ledger technology (DLT) security X.1400-X.1429 Application Security (2) Web security (2) Vulerability/state exchange Verview of cybersecurity Vulerability/state exchange Exchange of policies K.1520-X.1539 Event/incident/heuristics exchange X.1520-X.1559 Heuristics and information request X.1500-X.159 VL0DC OMPUTING SECURITY Overview of cloud computing security Verview of cloud computing security Vulerability design Cloud computing security design Cloud computing security design Cloud computing security design Cloud computing security design Cloud computing security QUANTUM COMMUNICATION Parametery of QKDN Security design for QKDN X.1700-X.1701 Quantum random number generator X.1700-X.1701 Quantum random number generator X.1700-X.1701 Security design for QKDN X.1710-X.1709 Mata protection X.1700-X.1701 Security design for QKDN X.1710-X.1719 Security techniques for QKDN X.1710-X.1719 Security bechiques for QKDN X.1700-X.1759 DATA SECURITY Big Data Security MT-2020 SECURITY X.1800-X.1819	Cybersocurity	X 1200 X 1220
Connering spanX.1250-X.1249Identity managementX.1250-X.1279SECURE APPLICATIONS AND SERVICES (2)X.1300-X.1309Emergency communicationsX.1310-X.1319Smart grid securityX.1310-X.1319Smart grid securityX.1330-X.1339Certified mailX.1340-X.1349Internet of things (IoT) securityX.1370-X.1349Internet of things (IoT) securityX.1400-X.1429Application Security (2)X.1400-X.1429Web security (2)X.1470-X.1439Overview of cybersecurityX.150-X.1519Vulnerability/state exchangeX.150-X.1539Event/incident/heuristics exchangeX.150-X.1549Vulnerability/state exchangeX.150-X.1549Event/incident/heuristics exchangeX.150-X.1549Event/incident/heuristics exchangeX.150-X.1549Cyber DefenceX.150-X.1559Cuber DefenceX.1500-X.1569Cuber Oreputing security designX.1600-X.1601Cloud computing security best practices and guidelinesX.1600-X.1639Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security best practices and guidelinesX.1600-X.1619Other cloud computing securityX.1600-X.1619Cloud computing security Dest practices and guidelinesX.1600-X.1619Cloud computing securityX.1600-X.1619Cloud computing securityX.1600-X.1619Cloud computing securityX.1600-X.1619Other cloud co	Constanting	X.1200 - X.1227 X.1220 - X.1227
SECURE APPLICATIONS AND SERVICES (2) Emergency communications X.1300–X.1309 Ubiquitous sensor network security X.1310–X.1319 X.1310–X.1319 X.1310–X.1339 Certified mail X.1340–X.1339 Internet of things (IoT) security X.1370–X.1399 Distributed ledger technology (DLT) security X.1370–X.1399 Distributed ledger technology (DLT) security X.1400–X.1459 Web security (2) X.1470–X.1459 Web security (2) X.1470–X.1459 Vulnerability/state exchange X.1500–X.1519 Vulnerability/state exchange X.1500–X.1519 Vulnerability/state exchange X.1500–X.1519 Heuristics and information request X.1560–X.1559 Heuristics and information request X.1560–X.1559 CLOUD COMPUTING SECURITY Overview of cloud computing security X.1500–X.1599 CLOUD COMPUTING SECURITY Overview of cloud computing security X.1500–X.1599 CLOUD COMPUTING SECURITY Overview of cloud computing security X.1600–X.1601 Cloud computing security design Cloud computing security design Cloud computing security methemation X.1600–X.1609 Cloud computing security Methemation X.1600–X.1701 Quantum random number generator X.1700–X.1701 Quantum random number generator X.1700–X.1701 Quantum random number generator X.1700–X.1701 Muantum random number generator X.1702–X.1709 Mata protection X.1710–X.1711 Security design for QKDN X.1710–X.1719 MIT-2020 SECURITY Big Data Security X.1819 MIT-2020 SECURITY	Identity magament	X.1250 - X.1249 X.1250 - X.1249
Energency communications X.1300-X.1309 Ubiquitous sensor network security X.1310-X.1319 Mart grid security X.1330-X.1339 Certified mail X.1330-X.1339 Internet of things (IoT) security X.1340-X.1349 Internet of things (IoT) security X.1370-X.1349 Internet of things (IoT) security X.1370-X.1349 Intelligent transportation system (ITS) security X.1370-X.1349 Distributed ledger technology (DLT) security X.1470-X.1429 Application Security (2) X.1450-X.1429 Vulnerability/state exchange X.1500-X.1519 Vulnerability/state exchange X.1520-X.1539 Event/incident/heuristics exchange X.1520-X.1539 Heuristics and information request X.1560-X.1549 Heuristics and information request X.1560-X.1559 CLOUD COMPUTING SECURITY Overview of cloud computing security X.1590-X.1599 CLOUD COMPUTING SECURITY Overview of cloud computing security design X.1600-X.1639 Cloud computing security uplementation X.1660-X.1659 Cloud computing security uplementation X.1660-X.1659 Cloud computing security uplementation X.1660-X.1659 Cloud computing security matches and guidelines X.1660-X.1659 Cloud computing security M.1680-X.1709 Terminologies X.1700-X.1709 Framework of QKDN security X.1700-X.1709 Framework of QKDN security X.1710-X.1710 Security design for QKDN X.1710-X.1719 Security design for QKDN X.1710-X.1719 Mata protection X.1700-X.1729 Mata protection X.1700-X.1729 Mata protection X.1700-X.1739 DATA SECURITY	Secure a del lo attonic and sedvices (2)	Λ.1230-Λ.1273
Energency communicationsX.1300-X.1309Ubiquitous sensor network securityX.1310-X.1319Smart grid securityX.1330-X.1339Certified mailX.1350-X.1339Internet of things (IoT) securityX.1350-X.1399Distributed ledger technology (DLT) securityX.1370-X.1399Distributed ledger technology (DLT) securityX.1470-X.149Application Security (2)X.1450-X.1459Web security (2)X.1470-X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500-X.1519Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1559Event/incident/heuristics exchangeX.1500-X.1559Identification and discoveryX.1570-X.1579Heuristics and information requestX.1560-X.1569Identification and discoveryX.1500-X.1599CLOUD COMPUTING SECURITYVoerview of cloud computing securityOverview of cloud computing securityX.1600-X.1601Cloud computing security beractices and guidelinesX.1640-X.1659Cloud computing security melementationX.1640-X.1679Other cloud computing securityX.1700-X.1710Quantum random number generatorX.1700-X.1710Pramework of QKDN securityX.1710-X.1719Security design for QKDNX.1712-X.1719Security techniques for QKDNX.1720-X.1729DATA SECURITYY.1750-X.1759Big Data SecurityX.1750-X.1759Data Security techniques for QKDNX.1720-X.1729DATA SECURITYY.1700-X.1719Big Data Security	Emergency communications	V 1200 V 1200
Dolquitous sensor network securityX.1310–X.1319Smart grid securityX.1330–X.1339Certified mailX.1340–X.1349Intenet of things (IoT) securityX.1370–X.1399Distributed ledger technology (DLT) securityX.1370–X.1399Distributed ledger technology (DLT) securityX.1400–X.1429Application Security (2)X.1470–X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500–X.1519Overview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1520–X.1559Heuristics and information requestX.1500–X.1559Identification and discoveryX.1570–X.1579Assured exchangeX.1500–X.1599CLOUD COMPUTING SECURITYX.1600–X.1601Cloud computing security implementationX.1602–X.1639Cloud computing security implementationX.1602–X.1639Cloud computing security implementationX.1600–X.1609QUANTUM COMMUNICATIONX.1700–X.1701Quantum random number generatorX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1729Paramework of QKDN securityX.170–X.1729DATA SECURITYX.1700–X.1719Security design for QKDNX.1720–X.1729DATA SECURITYX.1720–X.1739Big Data SecurityX.1750–X.1759Data protectionX.1720–X.1789IMT-2020 SECURITYX.180–X.1889	Emergency communications	$\Lambda.1300 - \Lambda.1309$ V 1210 V 1210
Smart grid securityX.1330-X.1339Certified mailX.1340-X.1349Internet of things (IoT) securityX.1340-X.1369Intelligent transportation system (ITS) securityX.1370-X.1399Distributed ledger technology (DLT) securityX.1400-X.1429Application Security (2)X.1400-X.1429Web security (2)X.1470-X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500-X.1519Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Exchange of policiesX.1500-X.1559Heuristics and information requestX.1500-X.1559Identification and discoveryX.1500-X.1579Assured exchangeX.1500-X.1589Cyber DefenceX.1500-X.1599CLOUD COMPUTING SECURITYX.1600-X.1601Cloud computing security designX.1600-X.1601Cloud computing security designX.1640-X.1659Cloud computing security best practices and guidelinesX.1640-X.1659Cloud computing security implementationX.1640-X.1659Other cloud computing securityX.1680-X.1799QUANTUM COMMUNICATIONX.1700-X.1701Quantum random number generatorX.1700-X.1701Pramework of QKDN securityX.1710-X.1711Security design for QKDNX.1720-X.1729DATA SECURITYX.1700-X.1799Data protectionX.1750-X.1759Data protectionX.1750-X.1759Data protectionX.1770-X.1789Material discoverial discoverial discoverial discoverial discoverial discoverial discoverial discoverial	Ubiquitous sensor network security	X.1310-X.1319 X.1320 X.1320
Certified mailX.1340-X.1349Internet of things (loT) securityX.1350-X.1369Intelligent transportation system (ITS) securityX.1470-X.1439Distributed ledger technology (DLT) securityX.1400-X.1429Application Security (2)X.1470-X.1459Web security (2)X.1470-X.1489Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1539Event/incident/heuristics exchangeX.1520-X.1539Event/incident/heuristics exchangeX.1500-X.1569Heuristics and information requestX.1500-X.1569Identification and discoveryX.1500-X.1579Assured exchangeX.1500-X.1579CLOUD COMPUTING SECURITYVorview of cloud computing securityOverview of cloud computing securityX.1600-X.1601Cloud computing security implementationX.1600-X.1639Cloud computing security best practices and guidelinesX.1600-X.1619Cloud computing security implementationX.1600-X.1619Other cloud computing securityX.1600-X.1619Cloud computing security implementationX.1600-X.1619Other cloud computing securityX.1600-X.1709Paramework of QKDN securityX.1700-X.1701Security design for QKDNX.1710-X.1711Security design for QKDNX.1720-X.1729DATA SECURITYX.1750-X.1759Data protectionX.1750-X.1759Data protectionX.1770-X.1789Maternet of QKDNX.1720-X.1729DATA SECURITYX.1800-X.1819	Smart grid security	X.1330–X.1339
Internet of things (101) securityX.130–X.1369Intelligent transportation system (ITS) securityX.1370–X.1399Distributed ledger technology (DLT) securityX.1400–X.1429Application Security (2)X.1450–X.1459Web security (2)X.1470–X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500–X.1519Overview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1550–X.1559Event/incident/heuristics exchangeX.1550–X.1559Heuristics and information requestX.1500–X.1569Identification and discoveryX.1500–X.1569CLOUD COMPUTING SECURITYX.1600–X.1601Cloud computing security designX.1600–X.1601Cloud computing security designX.1600–X.1601Cloud computing security best practices and guidelinesX.1600–X.1679Outor cloud computing securityX.1600–X.1679QUANTUM COMMUNICATIONX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1710–X.1711Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1700–X.1789Mata Data SecurityX.1700–X.1789IMT-2020 SECURITYX.1800–X.1819	Certified mail	X.1340–X.1349
Intelligent transportation system (11S) securityX.13/0+X.1399Distributed ledger technology (DLT) securityX.1400-X.1429Application Security (2)X.1450-X.1459Web security (2)X.1470-X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500-X.1519Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1500-X.1519Event/incident/heuristics exchangeX.1540-X.1549Exchange of policiesX.1550-X.1559Heuristics and information requestX.1500-X.1569Identification and discoveryX.1570-X.1579Assured exchangeX.1580-X.1589Cyber DefenceX.1590-X.1599CLOUD COMPUTING SECURITYX.1600-X.1601Cloud computing security designX.1600-X.1601Cloud computing security designX.1600-X.1601Cloud computing security implementationX.1600-X.1619Other cloud computing securityX.1600-X.1619QUANTUM COMMUNICATIONX.1700-X.1701Quantum random number generatorX.1700-X.1701Framework of QKDN securityX.1710-X.1711Security design for QKDNX.1712-X.1719Security techniques for QKDNX.1712-X.1759DATA SECURITYX.1700-X.1789Big Data SecurityX.1700-X.1781Big Data SecurityX.1700-X.1781Big Data SecurityX.1700-X.1781Big Data SecurityX.1700-X.1781Big Data SecurityX.1700-X.1781Security cetoniques for QKDNX.1700-X.1789DATA SECURITYX.1800-X.1819Cl	Internet of things (101) security	X.1350-X.1369
Distributed ledger technology (DL1) securityX.1400-X.1429Application Security (2)X.1450-X.1459Web security (2)X.1470-X.1489Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1520-X.1539Event/incident/heuristics exchangeX.1520-X.1549Exchange of policiesX.1550-X.1559Heuristics and information requestX.1570-X.1579Identification and discoveryX.1570-X.1579Assured exchangeX.1570-X.1579CLOUD COMPUTING SECURITYX.1600-X.1601Cloud computing security designX.1600-X.1601Cloud computing security designX.1600-X.1639Cloud computing security mplementationX.1600-X.1699QUANTUM COMMUNICATIONX.1700-X.1701Quantum random number generatorX.1700-X.1701TerminologiesX.1700-X.1701Security design for QKDNX.1712-X.1719Security techniques for QKDNX.1712-X.1719Big Data SecurityX.1700-X.1729DATA SECURITYX.1700-X.1789IMT-2020 SECURITYX.1800-X.1819	Intelligent transportation system (ITS) security	X.15/0-X.1399
Application Security (2)X.1450–X.1459Web security (2)X.1470–X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500–X.1519Overview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1520–X.1539Event/incident/heuristics exchangeX.150–X.1559Heuristics and information requestX.1560–X.1569Identification and discoveryX.1570–X.1579Assured exchangeX.1590–X.1599Cyber DefenceX.1590–X.1599CLOUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1600–X.1701Quantum random number generatorX.1700–X.1701Quantum random number generatorX.1700–X.1701Pramework of QKDN securityX.1710–X.1711Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1700–X.1759Data protectionX.170–X.1789IMT-2020 SECURITYX.1800–X.1819	Distributed ledger technology (DLT) security	X.1400–X.1429
Web security (2)X.1470–X.1489CYBERSECURITY INFORMATION EXCHANGEX.1500–X.1519Overview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1540–X.1549Exchange of policiesX.1550–X.1559Heuristics and information requestX.1560–X.1569Identification and discoveryX.1570–X.1579Assured exchangeX.1580–X.1589Cyber DefenceX.1590–X.1589CloUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1640–X.1659Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1710–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1700–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Application Security (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGEOverview of cybersecurityX.1500–X.1519Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1540–X.1549Exchange of policiesX.1550–X.1559Heuristics and information requestX.1560–X.1569Identification and discoveryX.1570–X.1579Assured exchangeX.1570–X.1579CLOUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1600–X.1609Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1709TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1712–X.1719Security design for QKDNX.1712–X.1719Security design for QKDNX.1712–X.1719Jotta SECURITYJ.1720–X.1739DATA SECURITYX.1700–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Web security (2)	X.1470–X.1489
Overview of cybersecurityX.1500-X.1519Vulnerability/state exchangeX.1520-X.1539Event/incident/heuristics exchangeX.1540-X.1549Exchange of policiesX.1550-X.1559Heuristics and information requestX.1550-X.1569Identification and discoveryX.1570-X.1579Assured exchangeX.1580-X.1589Cyber DefenceX.1580-X.1589CLOUD COMPUTING SECURITYX.1600-X.1601Cloud computing security designX.1602-X.1639Cloud computing security designX.1602-X.1639Cloud computing security implementationX.1660-X.1699QUANTUM COMMUNICATIONX.1600-X.1701TerminologiesX.1700-X.1701Quantum random number generatorX.1702-X.1709Framework of QKDN securityX.1711-X.1711Security design for QKDNX.1712-X.1719DATA SECURITYX.1700-X.1729DATA SECURITYX.1700-X.1789IMT-2020 SECURITYX.1700-X.1789IMT-2020 SECURITYX.1800-X.1819	CYBERSECURITY INFORMATION EXCHANGE	
Vulnerability/state exchangeX.1520–X.1539Event/incident/heuristics exchangeX.1540–X.1549Exchange of policiesX.1550–X.1559Heuristics and information requestX.1560–X.1569Identification and discoveryX.1570–X.1579Assured exchangeX.1580–X.1589Cyber DefenceX.1590–X.1599CLOUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1600–X.1701Quantum random number generatorX.1700–X.1701Framework of QKDN securityX.1711–X.1711Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1700–X.1799Data protectionX.170–X.1799Mt-2020 SECURITYX.1800–X.1819	Overview of cybersecurity	X.1500–X.1519
Event/incident/heuristics exchangeX.1540-X.1549Exchange of policiesX.1550-X.1559Heuristics and information requestX.1560-X.1569Identification and discoveryX.1570-X.1579Assured exchangeX.1580-X.1589Cyber DefenceX.1580-X.1589CLOUD COMPUTING SECURITYX.1600-X.1601Overview of cloud computing securityX.1600-X.1639Cloud computing security best practices and guidelinesX.1640-X.1659Cloud computing security implementationX.1660-X.1679Other cloud computing securityX.1600-X.1701QUANTUM COMMUNICATIONX.1700-X.1701TerminologiesX.1700-X.1701Quantum random number generatorX.1710-X.1711Security design for QKDNX.1712-X.1719Security techniques for QKDNX.1720-X.1729DATA SECURITYY.1700-X.1759Data SecurityX.1700-X.1759Data protectionX.1770-X.1789IMT-2020 SECURITYX.1800-X.1819	Vulnerability/state exchange	X.1520–X.1539
Exchange of policiesX.1550-X.1559Heuristics and information requestX.1560-X.1569Identification and discoveryX.1570-X.1579Assured exchangeX.1570-X.1579Cyber DefenceX.1590-X.1599CLOUD COMPUTING SECURITYX.1600-X.1601Overview of cloud computing securityX.1600-X.1601Cloud computing security designX.1602-X.1639Cloud computing security best practices and guidelinesX.1640-X.1659Cloud computing security implementationX.1660-X.1679Other cloud computing securityX.1680-X.1709QUANTUM COMMUNICATIONX.1700-X.1701Quantum random number generatorX.1710-X.1711Security design for QKDNX.1710-X.1719Security design for QKDNX.1720-X.1729DATA SECURITYX.1750-X.1759Data protectionX.170-X.1759Data protectionX.170-X.1789IMT-2020 SECURITYX.1800-X.1819	Event/incident/heuristics exchange	X.1540–X.1549
Heuristics and information requestX.1560–X.1569Identification and discoveryX.1570–X.1579Assured exchangeX.1580–X.1589Cyber DefenceX.1580–X.1589CLOUD COMPUTING SECURITYVerview of cloud computing securityOverview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1712–X.1719Security design for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Big Data SecurityX.1750–X.1759IMT-2020 SECURITYX.1800–X.1819	Exchange of policies	X.1550–X.1559
Identification and discoveryX.1570–X.1579Assured exchangeX.1580–X.1589Cyber DefenceX.1590–X.1599CLOUD COMPUTING SECURITYVOverview of cloud computing securityX.1600–X.1601Cloud computing security designX.1600–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONVTerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1720–X.1729DATA SECURITYVBig Data SecurityX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Heuristics and information request	X.1560–X.1569
Assured exchangeX.1580–X.1589Cyber DefenceX.1590–X.1599CLOUD COMPUTING SECURITYVOverview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1799QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYBig Data SecurityX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Identification and discovery	X.1570–X.1579
Cyber DefenceX.1590–X.1599CLOUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719DATA SECURITYBig Data SecurityX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Assured exchange	X.1580-X.1589
CLOUD COMPUTING SECURITYX.1600–X.1601Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Cyber Defence	X.1590–X.1599
Overview of cloud computing securityX.1600–X.1601Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1680–X.1699TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	CLÓUD COMPUTING SECURITY	
Cloud computing security designX.1602–X.1639Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1660–X.1679QUANTUM COMMUNICATIONX.1700–X.1701Quantum random number generatorX.1700–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Overview of cloud computing security	X.1600-X.1601
Cloud computing security best practices and guidelinesX.1640–X.1659Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Cloud computing security design	X.1602-X.1639
Cloud computing security implementationX.1660–X.1679Other cloud computing securityX.1660–X.1679QUANTUM COMMUNICATIONX.1680–X.1699TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Cloud computing security best practices and guidelines	X.1640-X.1659
Other cloud computing securityX.1680–X.1699QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Cloud computing security implementation	X 1660–X 1679
QUANTUM COMMUNICATIONX.1700–X.1701TerminologiesX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Other cloud computing security	X 1680-X 1699
Control Contro	OUANTUM COMMUNICATION	11.1000 11.10))
Quantum random number generatorX.1700–X.1701Quantum random number generatorX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Terminologies	X 1700-X 1701
Framework of QKDN securityX.1702–X.1709Framework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Data protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Quantum random number generator	X 1702_X 1700
Namework of QKDN securityX.1710–X.1711Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Big Data SecurityX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Framework of OKDN security	X = 1702 - X = 1703 X = 1710 $X = 1711$
Security design for QKDNX.1712–X.1719Security techniques for QKDNX.1720–X.1729DATA SECURITYX.1750–X.1759Big Data SecurityX.1770–X.1789DAta protectionX.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Francwork of QKDN Scoulty	A.1/10-A.1/11 V 1712 V 1710
Security techniques for QKDNX.1/20–X.1/29DATA SECURITYBig Data SecurityX.1750–X.1759Data protectionX.1770–X.1789X.1770–X.1789IMT-2020 SECURITYX.1800–X.1819	Security design for QKDN	A.1/12-A.1/19 V 1720 V 1720
DATA SECURITY X.1750–X.1759 Big Data Security X.1750–X.1759 Data protection X.1770–X.1789 IMT-2020 SECURITY X.1800–X.1819	DATA SECURITY	л.1/20-л.1/29
Dig Data Security X.1/50–X.1/59 Data protection X.1770–X.1789 IMT-2020 SECURITY X.1800–X.1819	DATA SECUKITY	V 1750 V 1750
IMT-2020 SECURITY X.1800–X.1819	Dig Data Security	A.1/30-A.1/39 X 1770 X 1790
IVI1-2020 SECUKITY X.1800–X.1819		A.1//U-A.1/89 X 1900 X 1910
	INIT-2020 SECUKITI	л.1800-А.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1379

Security requirements for roadside unit in intelligent transportation systems

Summary

Recommendation ITU-T X.1379 specifies the security requirements for roadside unit (RSU) in intelligent transportation systems (ITS) based on security threat analysis.

This Recommendation will help to guide vendors and operators of RSUs to adopt the appropriate security schemes to fulfil security requirements specified to protect RSUs from security risks and attacks from cyberspace thus to ensure the security of ITS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1379	2022-07-14	17	11.1002/1000/14994

Keywords

Intelligent transportation systems, roadside unit, security requirement.

i

^{*} To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, <u>http://handle.itu.int/11.1002/1000/11</u> <u>830-en</u>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

1	Scope		1
2	Referen	ces	1
3	Definiti	ons	1
	3.1	Terms defined elsewhere	1
	3.2	Terms defined in this Recommendation	2
4	Abbrevi	iations and acronyms	2
5	Conven	tions	2
6	Overvie	ew of RSU	2
7	Security	y threats to RSU	3
	7.1	Threats to RSU hardware	4
	7.2	Threats to RSU firmware/OS	4
	7.3	Threats to RSU application	4
	7.4	Threats to RSU data	4
8	Security	v requirements for RSU	5
	8.1	RSU hardware security requirements	5
	8.2	RSU firmware/OS security requirements	5
	8.3	RSU application security requirements	6
	8.4	RSU data security requirements	6
	8.5	Mapping of security threats to security requirements for RSU	7
Apper	ndix I – In	ntroduction of roadside unit (RSU)	9
Biblio	graphy		10

Recommendation ITU-T X.1379

Security requirements for roadside unit in intelligent transportation systems

1 Scope

Roadside unit (RSU) is a critical node in an intelligent transportation system (ITS) that enables vehicle-to-infrastructure (V2I) communication between on-board devices on vehicles and roadside infrastructures. RSU interacts with nearby vehicles, traffic control systems and a vehicle-to-everything (V2X) cloud service centre through various wired/wireless connections.

This Recommendation describes a function model and deployment issues of RSU for security analysis of RSU. It then identifies potential security threats to RSU before specifying the security requirements of the RSU to counter measure the security threats that are identified.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1371]	Recommendation ITU-T X.1371 (2020), Security threats to connected vehicles.
[ITU-T X.1372]	Recommendation ITU-T X.1372 (2020), Security guidelines for vehicle-to- everything (V2X) communication.
[ITU-T X.1374]	Recommendation ITU-T X.1374 (2020), Security requirements for external interfaces and devices with vehicle access capability.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1252]: Formalized process of verification that, if successful, results in an authenticated identity for an entity.

3.1.2 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.3 critical security parameters [b-ISO/IEC 19790]: Security related information whose disclosure or modification can compromise the security of a cryptographic module (e.g., secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors).

3.1.4 external interface [ITU-T X.1374]: A communication interface to provide connectivity between diverse external devices and the internal systems of a vehicle.

3.1.5 integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.6 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trust execution environment (TEE): An environment in which any code execution is trusted in authenticity and integrity, the assets are protected in confidentiality, and both assets and code are protected from unauthorized tracing and control through debug and test features.

NOTE – Adapted from [b-GPD SPE 009].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
AKA	Authentication and Key Agreement
IP	Internet Protocol
ITS	Intelligent Transportation Systems
OBU	On-Board Unit
OS	Operating System
RSU	Roadside Unit
TEE	Trust Execution Environment
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

6 Overview of RSU

Roadside unit (RSU) is a computing device located on the roadside that provides the connectivity support to the passing vehicles. The main function of the RSU is to facilitate the communication between vehicles and transportation infrastructure and other devices by transferring standardized ITS data.

The installation of the RSU depends upon local design, policies and the available infrastructure. To meet radio-communication objectives, RSU can be mounted directly on a traffic pole, a mast arm or installed in an adjacent cabinet.

Figure 1 shows a function model of the RSU. This model comprises four principal domains, i.e., the hardware, firmware / operating system (OS), application and the data. In the application domain, some applications are pre-installed by the application pre-installation module. The applications need to be updated by the application updating module. In the firmware/OS domain, the vulnerability recovery module aims to discover the vulnerabilities and recover normal states continuously. The permission restriction module aims to provide permission control for the user and the applications. The security configuration module provides the configurations for the security functions and the parameters.

Security of the RSU is closely related to these functions, therefore a security model of the RSU also contains four corresponding domains, i.e., the RSU hardware security, RSU firmware/OS security, RSU application security and the RSU data security.



Figure 1 – RSU function model

According to the RSU function model, there are many attack surfaces in each principal domain of the RSU. Compared with telecommunication network devices, the RSU has the following security characteristics:

- 1. Easier to be cracked: RSU may use open-source systems, which are relatively easy to be analysed and attacked. Systems and applications can be analysed more easily by extracting firmware rather than analysing assembly code.
- 2. More valuable to be attacked: RSU may involve financial applications, and even involve the customers' financial privacy, which may attract more attacks.
- 3. Higher protection costs: The cost of the security function design, software development, hardware production, certification of device and security management of RSUs will rise.
- 4. More attack surfaces: RSU may keep a lot of unnecessary network and system interfaces, while its physical environment is less controllable. RSU will face more attacks.

Depending on its function and usage environment, RSU is likely to encounter the following types of security threats: privacy disclosure, unauthorized access, system backdoor, firmware reverse, open-source component security vulnerabilities, insecure data encryption and security configuration.

An introduction to RSUs can be found in Appendix I.

7 Security threats to RSU

RSU is one of the core components of ITS which affects the safety of vehicles, pedestrians, and traffic. Based on the security model described above, security threats to RSU can be categorized as hardware security threats, firmware/OS security threats, application security threats and data security threats.

General security threats to connected vehicles are specified in [ITU-T X.1371]. Threats to external interfaces and devices with vehicle access capability are specified in [ITU-T X.1374]. In addition, the following threats are caused to the RSU because of insecure hardware or software design, and/or insecure configuration:

7.1 Threats to RSU hardware

Hardware-thr-1: If the debug interface of RSU is exposed, it can be used to break the device's working mechanism and to update the firmware.

Hardware-thr-2: A critical chip may be caused to enter an abnormal working state due to the input of a specific voltage.

Hardware-thr-3: Insecure chip packaging may lead to critical chips being attacked.

For other hardware interface threats, please refer to [ITU-T X.1374].

7.2 Threats to RSU firmware/OS

Firmware/OS-thr-1: The system is not updated in time, or the updated system contains security vulnerabilities. Once an old version of the operating system (OS) is equipped in the RSU, the possible and known system vulnerabilities or the defective security mechanisms in the process of system upgrades will cause the upgrade process to be attacked.

Firmware/OS-thr-2: Privilege abuse. The defective system permission control may be exploited by attackers to gain the system root privilege.

Firmware/OS-thr-3: Insecure firmware. If the integrity of the RSU firmware is not verified, the manipulated firmware can be executed.

Firmware/OS-thr-4: Defective system security configuration. The defective system configuration and authority allocation may increase the possibility of system intrusion, unauthorized remote control, and malicious firmware refresh.

Firmware/OS-thr-5: Firmware reverse engineering. The RSU may be tampered once the firmware is reversed.

For other firmware identified threats, please refer to [ITU-T X.1372].

7.3 Threats to RSU application

Application-thr-1: The pre-installed application is not updated in time, or the updated system contains security vulnerabilities. The known vulnerabilities or the insecure application upgrade process may make the upgrade process be attacked.

7.4 Threats to RSU data

Data-thr-1: If the firmware stores sensitive information such as passwords and secret keys, the leakage of sensitive information may make the device to be remotely controlled.

Data-thr-2: Improper data access control policies may cause data leakage.

Data-thr-3: For the RSU which supports external storage devices, data leakage may occur when the application software stores and transfers important data to the external storage devices.

Data-thr-4: For the RSU that supports peripheral transmission interfaces, the abuse of input and output functions may cause data leakage and malicious intrusion.

Data-thr-5: RSU may be led to abnormal operation status and data leakage, because of extreme weather (e.g., storm, hurricane), power failure, etc.

8 Security requirements for RSU

8.1 RSU hardware security requirements

Hardware-req-1: Physical protection to the enclosure of RSU is required to prevent being dismantled easily.

Hardware-req-2: Secure chip packaging is required to prevent the chip pin from being uncovered.

Hardware-req-3: Trust execution environment (TEE) is required to be supported to provide security features, such as isolated execution integrity of applications, etc.

Hardware-req-4: The cryptographic module in the RSU is required to support passivation mechanisms (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or physical damage).

Hardware-req-5: All plaintext (e.g., sensitive information) and critical security parameters contained in the cryptographic module is required to be zeroized, when the cover of RSU is removed during maintenance.

Hardware-req-6: The cryptographic module is required to provide the evidence of tampering (e.g., on the cover, enclosure, and seal) when the physical access to the cryptographic module is attempted.

Hardware-req-7: The cryptographic module is required to contain tamper-resistance and zeroized circuitry, if it contains removable covers or physical maintenance interfaces (e.g., universal serial bus (USB), RS-232 interface).

The requirements from Hardware-req-4 to Hardware-req-7 only apply to the physically implemented RSU cryptographic modules.

The hardware-assisted security requirements including a secure central processing unit, secure storage and crypto hardware acceleration of RSU could refer to [ITU-T X.1374].

8.2 RSU firmware/OS security requirements

Firmware/OS-req-1: The ability to upgrade firmware/OS automatically or manually is required.

Firmware/OS-req-2: The ability to verify the authenticity of firmware/OS upgrade is required.

Firmware/OS-req-3: When the firmware/OS upgrade process is interrupted, the ability to restart the upgrade process or revert to the pre-upgrade version is required.

Firmware/OS-req-4: The firmware/OS is recommended to have the ability to eliminate serious security vulnerabilities by means of patches or software updates. Security vulnerabilities are recommended to be fixed in time.

Firmware/OS-req-5: The ability to verify remote control requests is required to prevent unauthorized login.

Firmware/OS-req-6: The secure boot-up mechanism is recommended to prevent the firmware/OS start up without integrity verification.

Firmware/OS-req-7: System services are recommended to follow the principle of least privilege. The number of open ports is recommended to be minimized.

Firmware/OS-req-8: For systems with configurable functions, the ability to modify the default configuration is recommended. The security configurations are recommended to include modification of default identity, modification of authentication information, turn on and turn off configuration service, etc.

Firmware/OS-req-9: The secure communication protocol is recommended to prevent unauthorized remote management.

Firmware/OS-req-10: The important partition (boot, OS) is recommended to be configured as read-only mode.

Firmware/OS-req-11: For devices with a debug function, the privilege of a debug process is recommended to be severely restricted to prevent the abuse of privilege.

Firmware/OS-req-12: For devices with USB ports, the USB debug interfaces are recommended to be turned off or hidden by default; verification is required when turned on.

Firmware/OS-req-13: Obfuscation is required to prevent firmware reverse engineering.

8.3 **RSU application security requirements**

Application-req-1: The function of secure encryption of sensitive information is required; explicitly recording sensitive information in logs and configuration files are prohibited.

Application-req-2: The ability to upgrade a pre-installed application from an official site by default is recommended; the data integrity and source installation package is recommended to be verified.

Application-req-3: Third-party libraries with known vulnerabilities are prohibited from being included in the source code.

Application-req-4: The use of a hard-coded password is prohibited.

Application-req-5: The ability to restrict remote application access to the server based on an access control list (ACL) is recommended.

Application-req-6: The ability to restrict an important application (e.g., C-V2X related) to be uninstalled is recommended.

8.4 **RSU data security requirements**

Data-req-1: The ability to protect sensitive data in the process of generating, storing, transmitting, destroying, backing up and recovering is required.

Data-req-2: The ability to verify the user's privilege is required when the user operates sensitive data.

Data-req-3: The application context file (including configuration files, databases, cookies, etc) is prohibited from storing the database password, FTP service password, login password, external system interface authentication password and other sensitive data.

Data-req-4: For devices which are remotely managed, the access to the management and configuration profiles without authentication is prohibited. The log of the authentication process is recommended to include the user account, login status, login time, and the user's IP address.

Data-req-5: The ability to protect sensitive data is required during transmission.

Data-req-6: Unexpected shut down, restart and file system collapse are recommended to be logged automatically.

Data-req-7: For systems supporting multiple accounts, the ability to isolate sensitive information from other data is recommended.

Data-req-8: The ability to reset the password for the RSU user account is recommended.

Data-req-9: The configuration files in the RSU are recommended to enforce digital signatures to prevent unauthorized modifications.

Data-req-10: The ability to restrict remote access based on an Internet protocol (IP) ACL is recommended.

Data-req-11: The ability to automatically save data is recommended to prevent data loss from abnormal power cuts.

Data-req-12: The ability to support public key certificates is required to implement authenticity, integrity, confidentiality and replay attack protection.

Data-req-13: The ability to support 4G/5G communication security mechanisms (e.g., authentication and key agreement (AKA), encryption and integrity protection in Uu interface [b-3GPP TS 23.501]) is recommended.

Data-req-14: The ability to support a certificate-based security mechanism in the application domain to implement secure communication between the RSU and cloud is recommended.

Data-req-15: The ability to support authentication, integrity protection, optional confidentiality and prevent replay attack is required when communicating with other devices through the Ethernet or an RS-232 interface [b-ITU-T V.24].

Data-req-16: RSU is recommended to support real-time queries and reports of the running status. The queries and reports are recommended to include connection status, fault status, working mode, power status, etc.

Data-req-17: RSU is recommended to report and process the fault incident. The information about the fault incident is recommended to be stored and reported in a unified format.

8.5 Mapping of security threats to security requirements for RSU

In summary, the mapping of different security threats described in clause 7 to their corresponding requirements described above in clause 8 are shown in the tables below:

- Table 1 is the mapping of the hardware security threats to the RSU hardware security requirements,
- Table 2 is the mapping of the firmware/OS security threats to the RSU firmware/OS security requirements,
- Table 3 is the mapping of the application security threats to the RSU application security requirements, and
- Table 4 is the mapping of the data security threats to the RSU data security requirements.

	Hardware-thr-1	Hardware-thr-2	Hardware-thr-3
Hardware-req-1	\checkmark		
Hardware-req-2			
Hardware-req-3			
Hardware-req-4		\checkmark	\checkmark
Hardware-req-5		\checkmark	
Hardware-req-6		\checkmark	
Hardware-req-7		\checkmark	

 Table 1 – Hardware security threats and requirements

 Table 2 – Firmware/OS security threats and requirements

	Firmware/ OS-thr-1	Firmware/ OS-thr-2	Firmware/ OS-thr-3	Firmware/ OS-thr-4	Firmware OS-thr-5
Firmware/OS-req-1	\checkmark				
Firmware/OS-req-2	\checkmark				

	Firmware/ OS-thr-1	Firmware/ OS-thr-2	Firmware/ OS-thr-3	Firmware/ OS-thr-4	Firmware OS-thr-5
Firmware/OS-req-3	\checkmark				
Firmware/OS-req-4	\checkmark				
Firmware/OS-req-5		\checkmark			
Firmware/OS-req-6			\checkmark		
Firmware/OS-req-7				\checkmark	
Firmware/OS-req-8				\checkmark	
Firmware/OS-req-9		\checkmark			
Firmware/OS-req-10		\checkmark			
Firmware/OS-req-11		\checkmark			
Firmware/OS-req-12				\checkmark	
Firmware/OS-req-13					

Table 2 – Firmware/OS security threats and requirements

Table 3 – Application security threats and requirements

	Application-	Application-	Application	Application	Application	Application
	req-1	req-2	-req-3	-req-4	-req-5	-req-6
Application-thr-1	\checkmark	$\overline{\mathbf{v}}$				

Table 4 – Data security threats and requirements

	Data-thr-1	Data-thr-2	Data-thr-3	Data-thr-4	Data-thr-5
Data-req-1	\checkmark				
Data-req-2	\checkmark				
Data-req-3	\checkmark				
Data-req-4		\checkmark			
Data-req-5		\checkmark			
Data-req-6					\checkmark
Data-req-7		\checkmark			\checkmark
Data-req-8		\checkmark			
Data-req-9		\checkmark			
Data-req-10		\checkmark			
Data-req-11					\checkmark
Data-req-12				\checkmark	
Data-req-13				\checkmark	
Data-req-14				\checkmark	
Data-req-15			\checkmark	\checkmark	
Data-req-16			\checkmark		\checkmark
Data-req-17			\checkmark	\checkmark	\checkmark

Appendix I

Introduction of roadside unit (RSU)

(This appendix does not form an integral part of this Recommendation.)

RSU is a wireless communication transceiver that is mounted along a road or a pedestrian passageway. RSUs broadcast data to on-board units (OBUs) or exchanges data with OBUs in their communication zone. OBUs are devices located in vehicles to collect data from the vehicle and/or provide an interface through which intelligent transportation systems (ITS) services, e.g., travel information and warnings, can be provided to the driver. RSU also provides channel assignments and operating instructions to OBUs in their communication zone, when required. RSUs prepare and transmit messages to the vehicles and receive messages from the vehicles, for the purpose of supporting vehicle-to-infrastructure (V2I) applications [b-FHWA-JPO-17-433].

RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or hand-carried unit is stationary. Furthermore, an RSU operating under this part is restricted to the location where it is licensed to operate. However, portable or handheld RSUs are permitted to operate where they do not interfere with a licensed operation.

Figure I.1 shows an interoperation relationship of the RSU. RSU is related to roadside traffic equipment, pedestrian, OBU and the application platforms.



Figure I.1 – Interoperation relationship of the RSU

Bibliography

[b-ITU-T X.800]	Recommendation ITU-T X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.
[b-ITU-T X.1252]	Recommendation ITU-T X.1252 (2021), Baseline identity management terms and definitions.
[b-ITU-T V.24]	Recommendation ITU-T V.24 (2000), <i>List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).</i>
[b-3GPP TS 23.501]	3GPP TS 23.501, version 16.1.0 (2019), <i>System architecture for the 5G</i> <i>System (5GS)</i> . < <u>https://portal.3gpp.org/desktopmodules/SpecificationSystemicationDetails.aspx?specificationId=3144</u> >
[b-FHWA-JPO-17-433]	FHWA-JPO-17-433 (2017), United States Department of Transportation, An Overview of USDOT Connected Vehicle Roadside Unit Research Activities. < <u>https://rosap.ntl.bts.gov/view/dot/34763></u>
[b-GPD SPE 009]	GPD_SPE_009 (2011), <i>GlobalPlatform Device Technology</i> , <i>TEE System</i> <i>Architecture</i> . < <u>https://globalplatform.org/specs-library/tee-system-architecture/></u>
[b-ISO/IEC 19790]	ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules.
	<https: 52906.html="" standard="" www.iso.org=""></https:>
[b-ISO/IEC 27000]	ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary.
	<https: 73906.html="" standard="" www.iso.org=""></https:>

SERIES OF ITU-T RECOMMENDATIONS

Series A Organization of the work of ITU-T

- Series D Tariff and accounting principles and international telecommunication/ICT economic and policy issues
- Series E Overall network operation, telephone service, service operation and human factors
- Series F Non-telephone telecommunication services
- Series G Transmission systems and media, digital systems and networks
- Series H Audiovisual and multimedia systems
- Series I Integrated services digital network
- Series J Cable networks and transmission of television, sound programme and other multimedia signals
- Series K Protection against interference
- Series L Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
- Series M Telecommunication management, including TMN and network maintenance
- Series N Maintenance: international sound programme and television transmission circuits
- Series O Specifications of measuring equipment
- Series P Telephone transmission quality, telephone installations, local line networks
- Series Q Switching and signalling, and associated measurements and tests
- Series R Telegraph transmission
- Series S Telegraph services terminal equipment
- Series T Terminals for telematic services
- Series U Telegraph switching
- Series V Data communication over the telephone network
- Series X Data networks, open system communications and security
- Series Y Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
- Series Z Languages and general software aspects for telecommunication systems