ITU Kaleidoscope 2013
Building Sustainable Communities

Telebiometric Information Security and Safety Management

Phillip H. Griffin
Information Security Consulting
phil@phillipgriffin.com

Kyoto, Japan
22-24 April 2013

The Challenge

Assess standardization required so that cities can enhance their social, economic, and environmental sustainability by using Information and Communications Technologies

Biometrics, Telecommunications

Human-oriented technologies

Security, Privacy, Safety

Human values

Suggest New Areas For Standardization 💡

New Standardization

Telebiometric System Heartbeat

Monitor, alert, continuously improve telebiometric an information security & safety management program

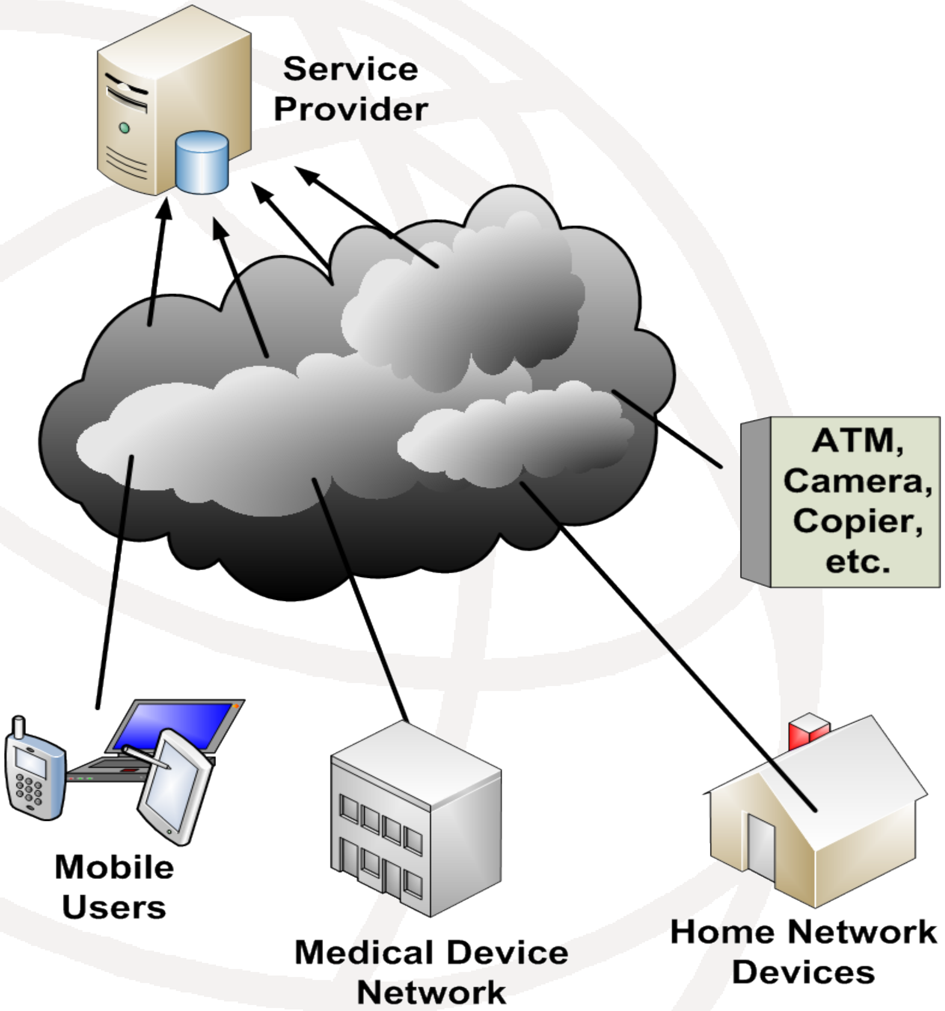
Cryptographic Message Syntax (CMS)

Valid ASN.1 – BER, PER, XER – SC 27 based

Signcryption CMS Type

Small, fast, efficient signature + encryption

System Heartbeat



Cryptographic Message Syntax

"a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes" - RSA Laboratories

- ❑ Defined by RSA Security in the early 1990s
- ❑ PKCS #7 (Public Key Cryptography Standard 7)
- ❑ Adopted by IETF to support secure email - S/MIME
- ❑ Needed in many biometric & security standards
- ❑ *No normative, valid, international standard exists!*

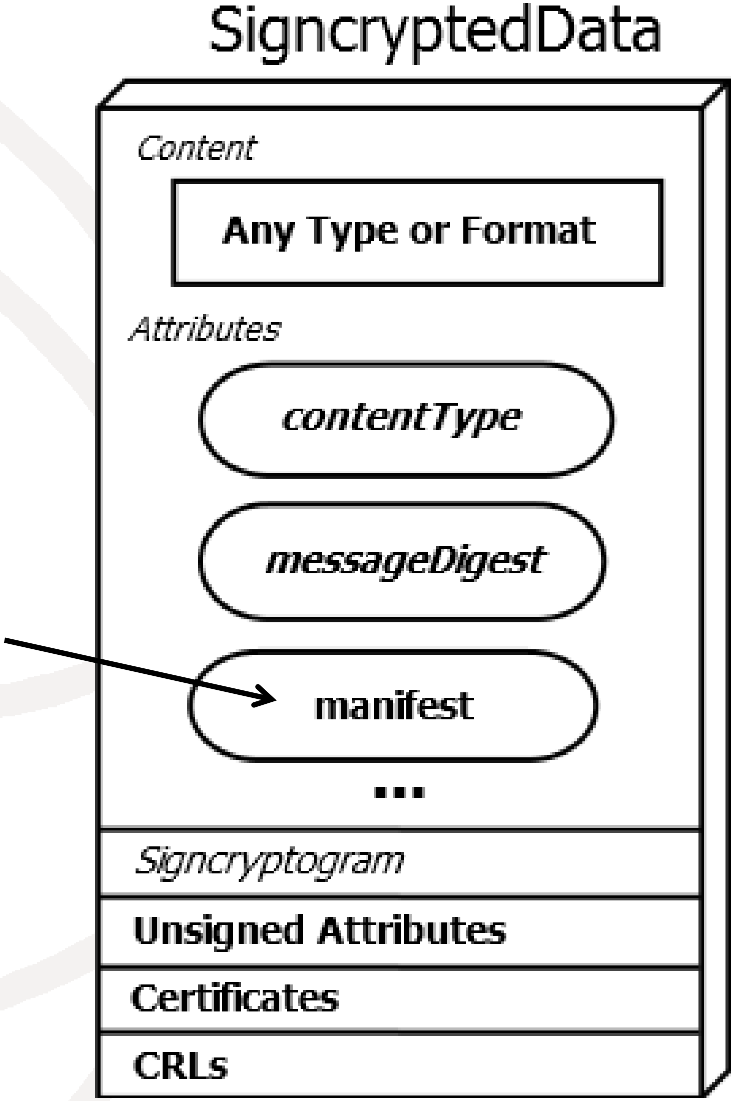
Signcryption CMS Type

ID360: Global Forum on Identity

Schema similar to SignedData

One processing mode supports field-level signcryption within a signed object & signed attributes

Attributes: Defined by any group with a need in any type or format



Summary

Telebiometric System Heartbeat

Need a standardized, extensible, CMS protected message to enable vendor neutral solutions

Cryptographic Message Syntax (CMS)

Need a modern, correct, international CMS based on ISO/IEC Standards | ITU-T Recommendations

CMS Signcryption Support

Need a *SigncryptedData* type to support the use of efficient ISO/IEC 29150 techniques in CMS

Questions?

phil@phillipgriffin.com +1 919 291 0019 Skype: phil.griffin