ITU-T Q10/17

Identity Summit
Geneva
December 10, 2010

Privacy Management Standards: What They Are and Why They Are Needed Now

John Sabo
Director Global Government Relations

Chair, OASIS IDtrust Member Section Steering Committee and Co-Chair OASIS PMRM TC

Privacy Basics: Fair Information Principles/Practices

- **Accountability**
- **Notice**
- **Consent**
- **Collection Limitation**
- **Use Limitation**
- **Disclosure**
- **Access & Correction**
- **Security/Safeguards**

- **Data Quality**
- **Enforcement**
- **Openness**

- **Anonymity**
- **Data Flow**
- **Sensitivity**

Global Privacy Principles/Practices
- similarities…but no policy standardization

Analysis of Privacy Principles: An Operational Study" - 2007
International Security Trust and Privacy Alliance (ISTPA)

OECD Guidelines – 1980

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- **Security Safeguards**
- Openness
- Individual Participation
- Accountability

CSA Model Code for Protection of Personal Information – 1996

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- **Safeguards**
- Openness
- Individual Access
- Challenging Compliance

APEC Privacy Framework – 2005

- Preventing Harm
- Notice
- Collection Limitation
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- **Security Safeguard**
- Access and Correction
- Accountability

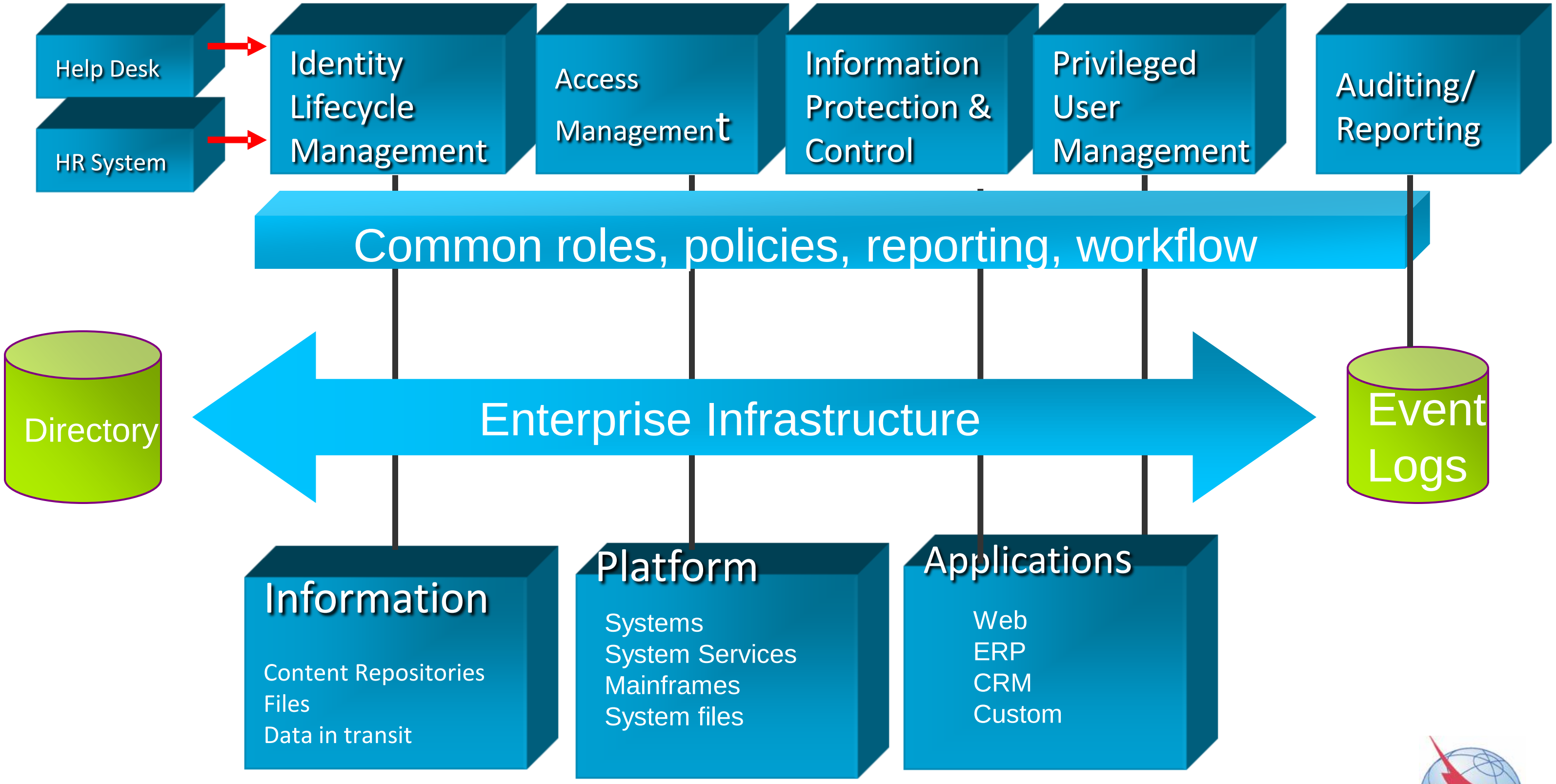
Used with Permission, International Security Trust and Privacy Alliance (ISTPA)

By Contrast: Rich Security Standardization and Technologies

- Fundamental Security Services
  - “Confidentiality, Data integrity, Availability”
- Plethora of Standards, such as
  - ISO/IEC 27001/2:2005
  - NIST FIPS 140-2 (crypto modules), FIPS-197 (AES), Special Publications
  - SAML 2.0
  - PCI-DSS
- Rich and Mature Discipline – Crypto, IAM, DLP…
- Many Mechanisms/Technologies/Solutions/Products/Services
- Expanding focus on IAM, federation, cloud

Policy-Driven

- Recognizing need for extensible models including policy-mapping, federated certification regimes, cloud interoperability



Privacy?… New Challenges

Social Networking

E-Government

Health IT

Smart Grid

Cloud Computing

Internet of Things

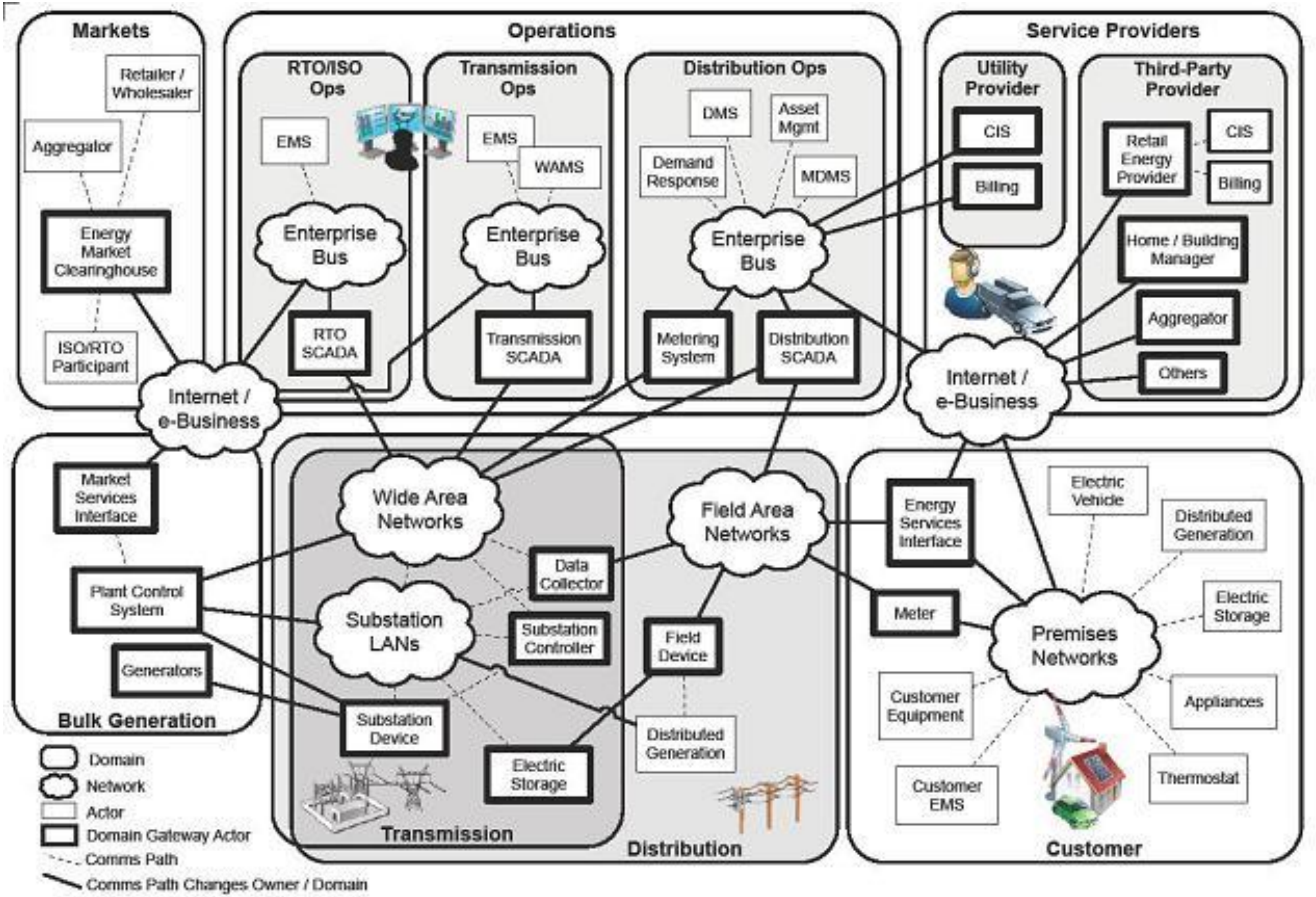
Location-based Applications

Aggregated/Inferred Personal Information

….

Example: *Smart Grid*

NIST Smart Grid Conceptual Model



Source: 27 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

Novel Smart Grid Risk Exposures

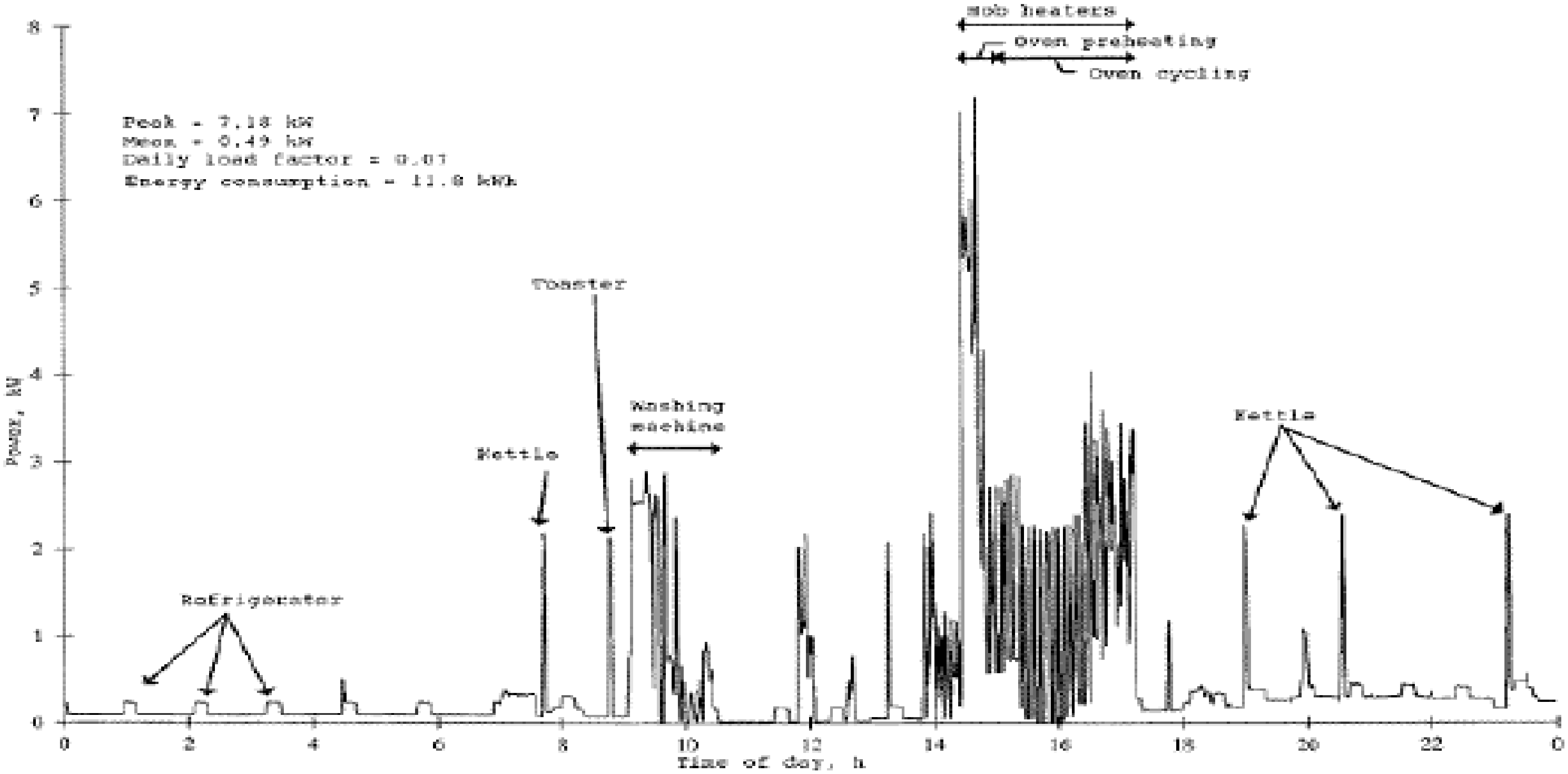


Figure 5-1 Power Usage to Personal Activity Mapping [30]

30. Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies, Spring 2009, at page 3*

NIST Smart Grid Report

- NIST Interagency Report - NISTIR 7628
- Smart Grid Interoperability Panel – Cyber Security Working Group
- Three volume report - published August 2010
- http://csrc.nist.gov/publications

Volume 1 – NISTIR 7628

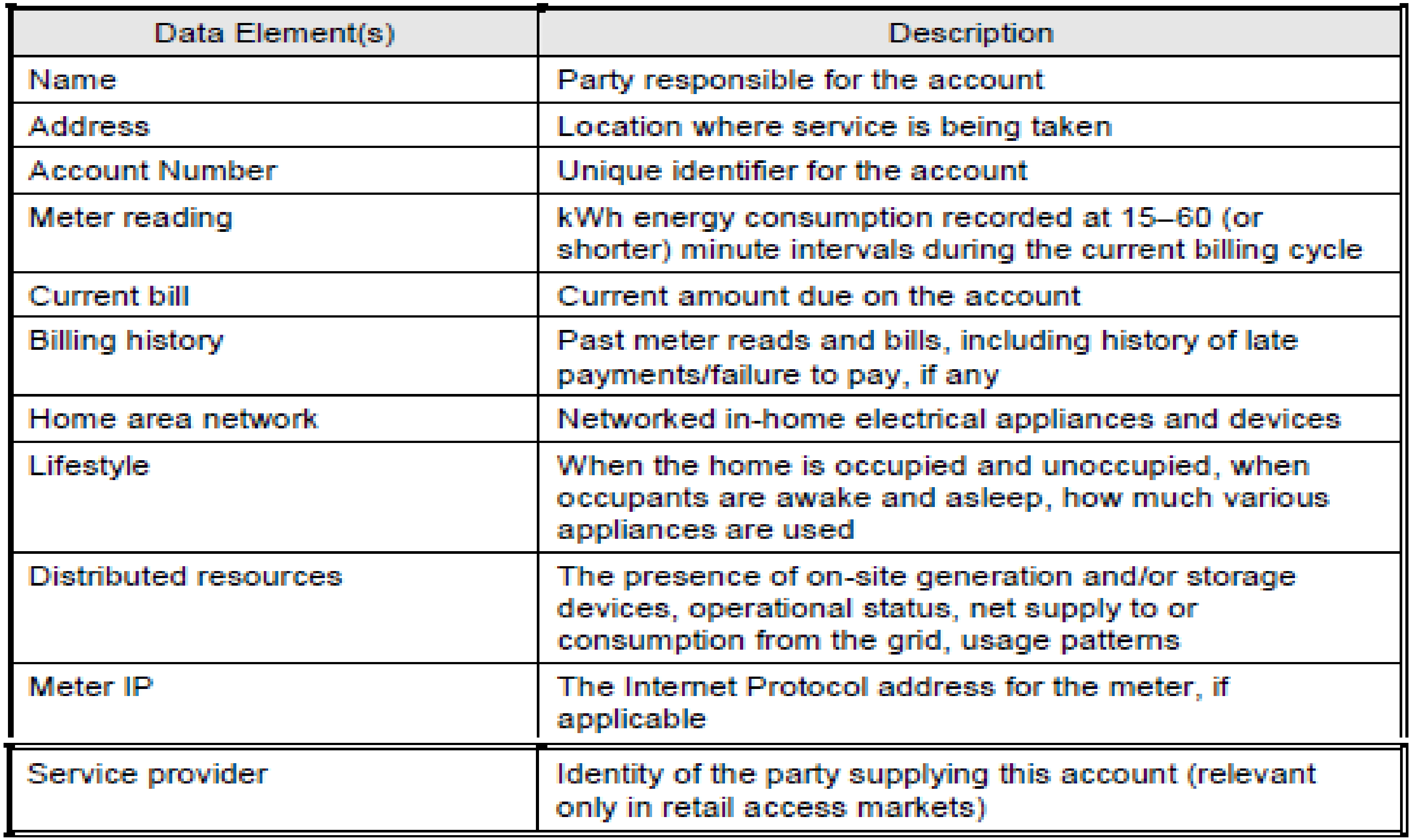
- Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - Chapter 1 – *Cyber Security*
  - Chapter 2 – *Logical Architecture - focuses on a short-term view (1–3 years) of the Smart Grid*
  - Chapter 3 – *High Level Security Requirements for each of the 22 logical interface categories*
  - Chapter 4 – *Cryptography and Key Management - identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid*

Volume 2 - NISTIR 7628

- Privacy and the Smart Grid
- Chapter 5 – *Privacy and the Smart Grid includes*
  - *privacy impact assessment for the Smart Grid with a discussion of mitigating factors.*
  - *potential privacy issues that may occur as new capabilities are included in the Smart Grid.*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*

Smart Grid Privacy Risk Areas

Table 5-1 Information potentially available through the Smart Grid



Data Element(s)	Description
Name	Party responsible for the account
Address	Location where service is being taken
Account Number	Unique identifier for the account
Meter reading	kWh energy consumption recorded at 15–60 (or shorter) minute intervals during the current billing cycle
Current bill	Current amount due on the account
Billing history	Past meter reads and bills, including history of late payments/failure to pay, if any
Home area network	Networked in-home electrical appliances and devices
Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used
Distributed resources	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
Meter IP	The Internet Protocol address for the meter, if applicable
Service provider	Identity of the party supplying this account (relevant only in retail access markets)

What is Missing?

- NISTR 7628 addresses residential users and their data
- Emphasis in the privacy chapter on consumer and enterprise privacy policy, privacy impact assessments, and privacy risk
- Privacy concerns for commercial, industrial, and institutional energy consumers will be addressed later “based on the pace of Smart Grid evolution”

By contrast - Volume 1 (security) is a detailed 289-page report with extensive references to smart grid architectures and technical security standards

What is Needed?

- **Operational Model for Privacy Management**
  - addressing the assured, consistent collection, minimization, processing, communication, use and disposition of PI and PII throughout its life cycle
  - Implementing data protection principles/practices, policy requirements, and the preferences of the individual/data subject
- **Lifecycle Model for Privacy Management**
  - applicable throughout the PI life cycle
  - all actors, systems, and networks that "touch" the information
  - an abstract model enabling lifecycle privacy management

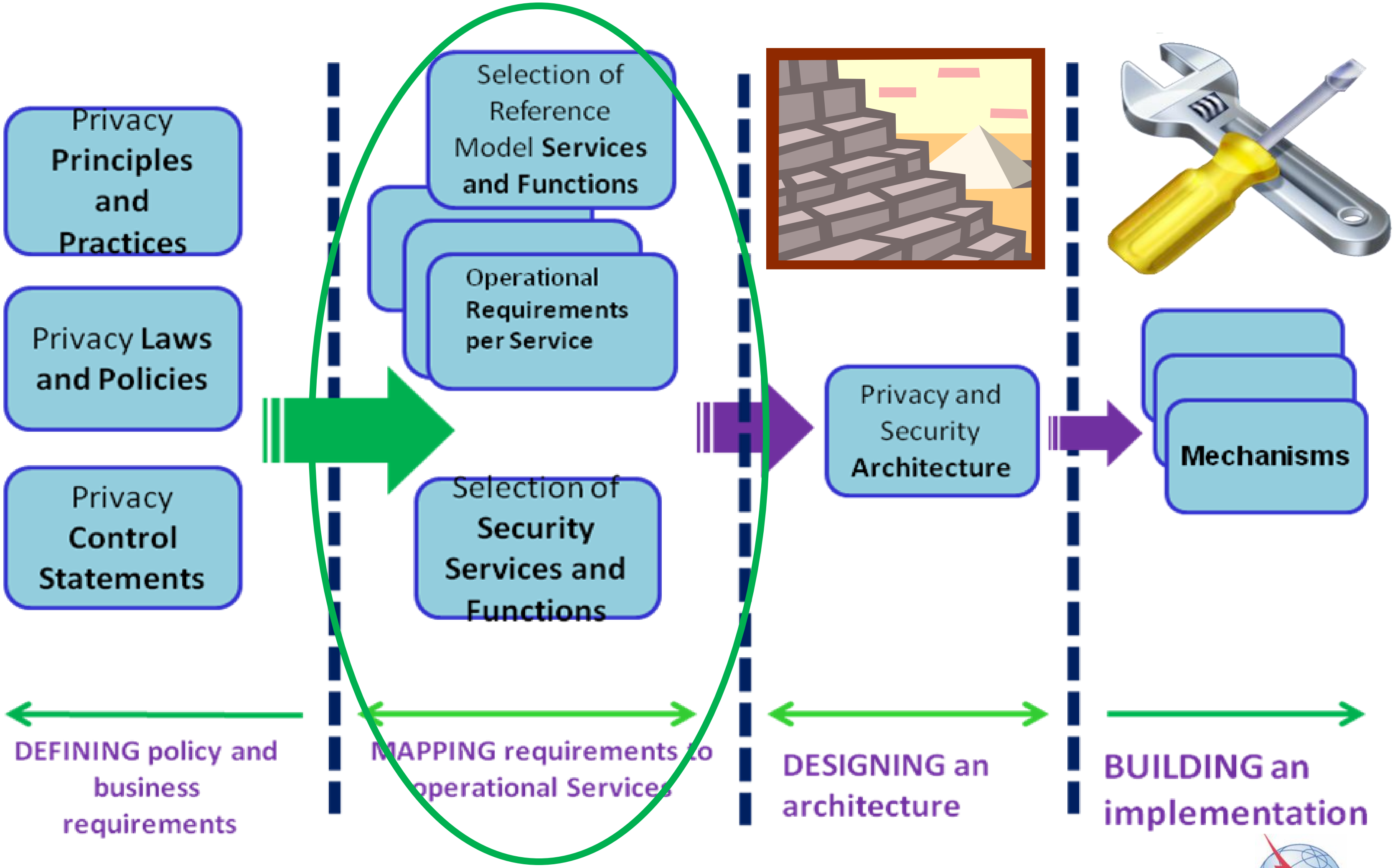
OASIS Privacy Management Reference Model Technical Committee

- Starting Point : the Privacy Reference Model v 2.0 contributed by the International Security Trust and Privacy Alliance (ISTPA)
- OASIS PMRM TC formally announced June 27 – first meeting September 8
- Deliverables include
  - the Reference Model
  - one or more use cases utilizing the PMRM
  - one or more formal methodologies for expressing use cases
  - profiles of the PMRM applied to selected specific environments (such as Cloud Computing, Health IT, e-Gov, and/or the Smart Grid)
  - linkages to security services

Key Components of Contributed Model

- Set of 10 privacy services + security and relationship to privacy requirements derived from principles/practices/policies
- Service definitions
- Set of unique functions for each service
- Syntax for invoking services
- Generic use case
- Linkages to security services

Where Does the Reference Model Fit?



Privacy **Principles and Practices**

Privacy **Laws and Policies**

Privacy **Control Statements**

Selection of Reference Model **Services and Functions**

Operational **Requirements per Service**

Selection of **Security Services and Functions**

Privacy and Security **Architecture**

Mechanisms

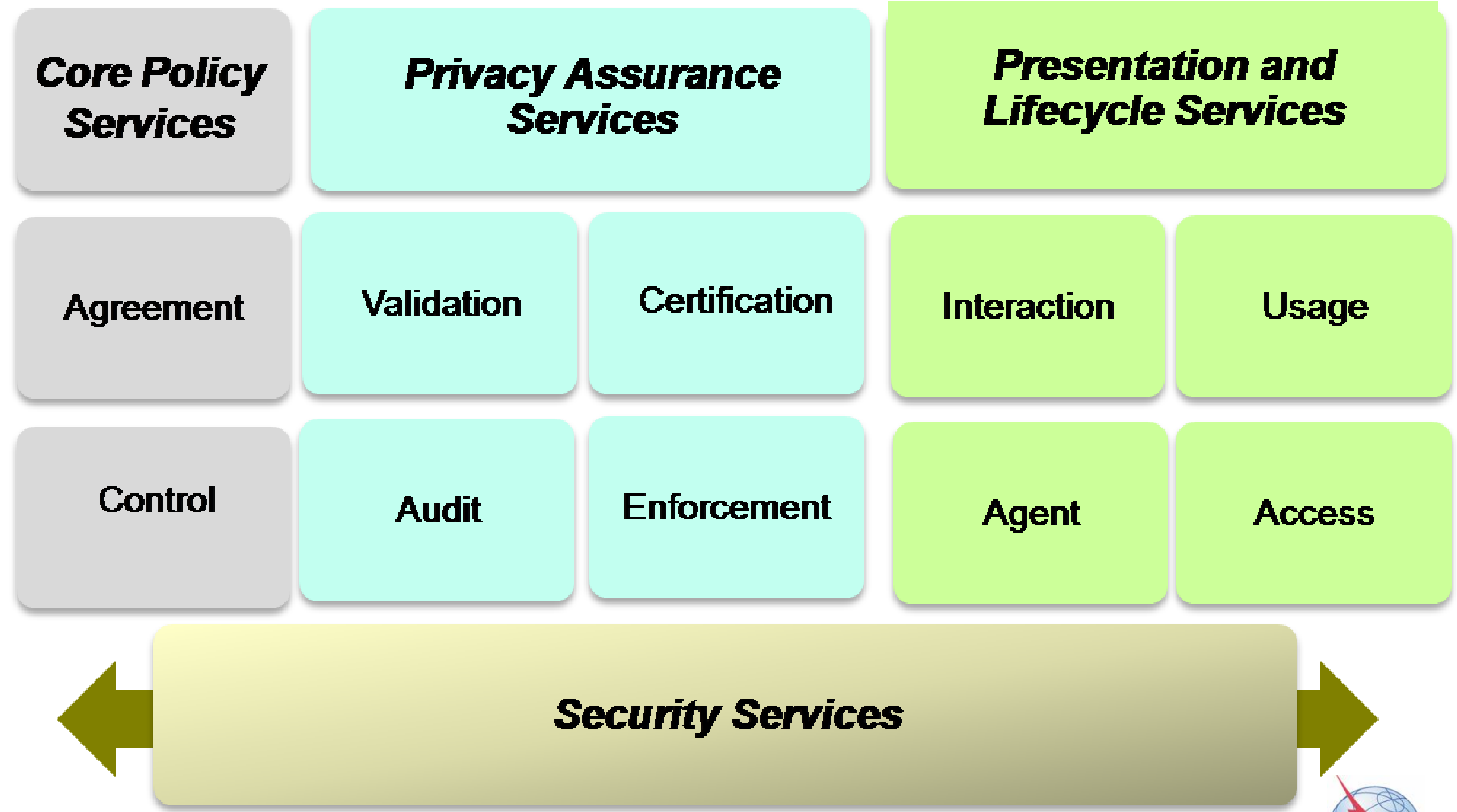
DEFINING policy and business requirements

MAPPING requirements to operational Services

DESIGNING an architecture

BUILDING an implementation

Privacy Reference Model



Core Policy Services	***Privacy Assurance Services***		***Presentation and Lifecycle Services***	
Agreement	Validation	Certification	Interaction	Usage
Control	Audit	Enforcement	Agent	Access

Security Services

Privacy Management Reference Model Services

- **Core Policy Services**
  - **Agreement** - agreements, options, permissions
  - **Control** - policy instantiation, data management

- **Presentation and Lifecycle Services**
  - **Interaction** - manages data/preferences/notice
  - **Agent** - software that carries out processes
  - **Usage** - lifecycle data use, aggregation, anonymity
  - **Access** - individual review/updates to PI

- **Privacy Assurance Services**
  - **Certification** - credentials, trusted processes
  - **Audit** - verifiable lifecycle accountability
  - **Validation** - quality and suitability of PI
  - **Enforcement** **-** including redress for violations

Concluding Points

- Cloud computing, smart grid, and other rapidly-evolving and innovative technologies and business practices are outpacing policy development and compliance regimes
  - **A continuum of technical standardization is necessary – from abstract, framework levels down to specific protocol and profile levels**
- The policy community – lawmakers and regulators – have a role, but will not achieve international consensus covering all data protection domains
  - **Even with abstract macro-level consensus, privacy requirements must operate at the level of data and rule-sets**
- A privacy management model is needed as a template to support use cases for specific infrastructures and business systems and policy complexity
  - **Privacy policies require significantly more granular, technical support in underlying networked systems over an indefinite information lifecycle**
- Policy management standardization is hugely important
  - **This is not about compliance – it is about configurable, standards-based technical management mechanisms operating in dynamic, rapidly-changing environments**

Thank you.

John.t.sabo@ca.com