

Building a Data Protection and Privacy Model for Cloud-Based Infrastructures

John Sabo, CISSP

Director Global Government Relations

CA Technologies

Chair, OASIS IDtrust Member Section Steering Committee

4th INTERNATIONAL CONFERENCE
25 26 27 JANUARY 2011 | BRUSSELS
BELGIUM
**COMPUTERS, PRIVACY &
DATA PROTECTION**



World Economic Forum 2009 -2010 Study on Cloud Computing Benefits and Barriers

—Economic Benefits

- Entrepreneurship; create new businesses, jobs
- Platform for innovation; accelerate innovation
- Increase IT efficiency and IT flexibility
- Business/technology leapfrogging opportunities in developing countries

— But...Major Barriers

- Privacy (63%)
- Data governance (e.g. data ownership, cross-border data transfer, etc. (56%)
- Security (50%)



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The Research Study is in second year – new findings and recommendations at January 2011 WEF Davos meeting

“Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation”

- Published by the World Economic Forum in early 2010 – see www.weforum.org
- Key Recommendations:
 - Improve transparency and provide clarification, e.g. government to prepare guidelines for existing legislation and data exchange; industry to provide clarity on how meta data is structured
 - Educate citizens on the implications, benefits and risks of cloud computing
 - Increase investment in R&D on security- and privacy-enhancing technologies
 - Work on harmonization and clarity of privacy and data processing regulations

ENISA Cloud Computing Study: “Benefits, Risks and Recommendations for Information Security”

— Privacy included in the November 2009 study – see www.enisa.europa.eu

- How best to support the minimum data protection standards and privacy certification schemes common **across the globe** and at least all the member States
- **International differences** in relevant regulations, including data protection and privacy
- Legal means to facilitate the smooth functioning of **multi-national** cloud infrastructures
- **Transparency:** privacy preserving data provenance systems, e.g., tracing data end-to-end through systems
- **Automated means** to mitigate problems with different jurisdictions



Cloud Computing :Jurisdictional Differences in Global Privacy Laws, Regulations, Policies

- Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
- Provincial laws and regulations
- The Privacy Act of 1974 (U.S.)
- OECD Privacy Guidelines
- UN Guidelines Concerning Personalized Computer Files
- EU Data Protection Directive 95/46/EC
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- International Labour Organization (ILO) Code of Practice on the Protection of Workers' Personal Data
- US FTC statement of Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Australian Privacy Act – National Privacy Principles
- California Senate Bill 1386, “Security Breach Notification”
- AICPA/CICA GAPP
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework

Global Privacy Principles/Practices - similarities...but no 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

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

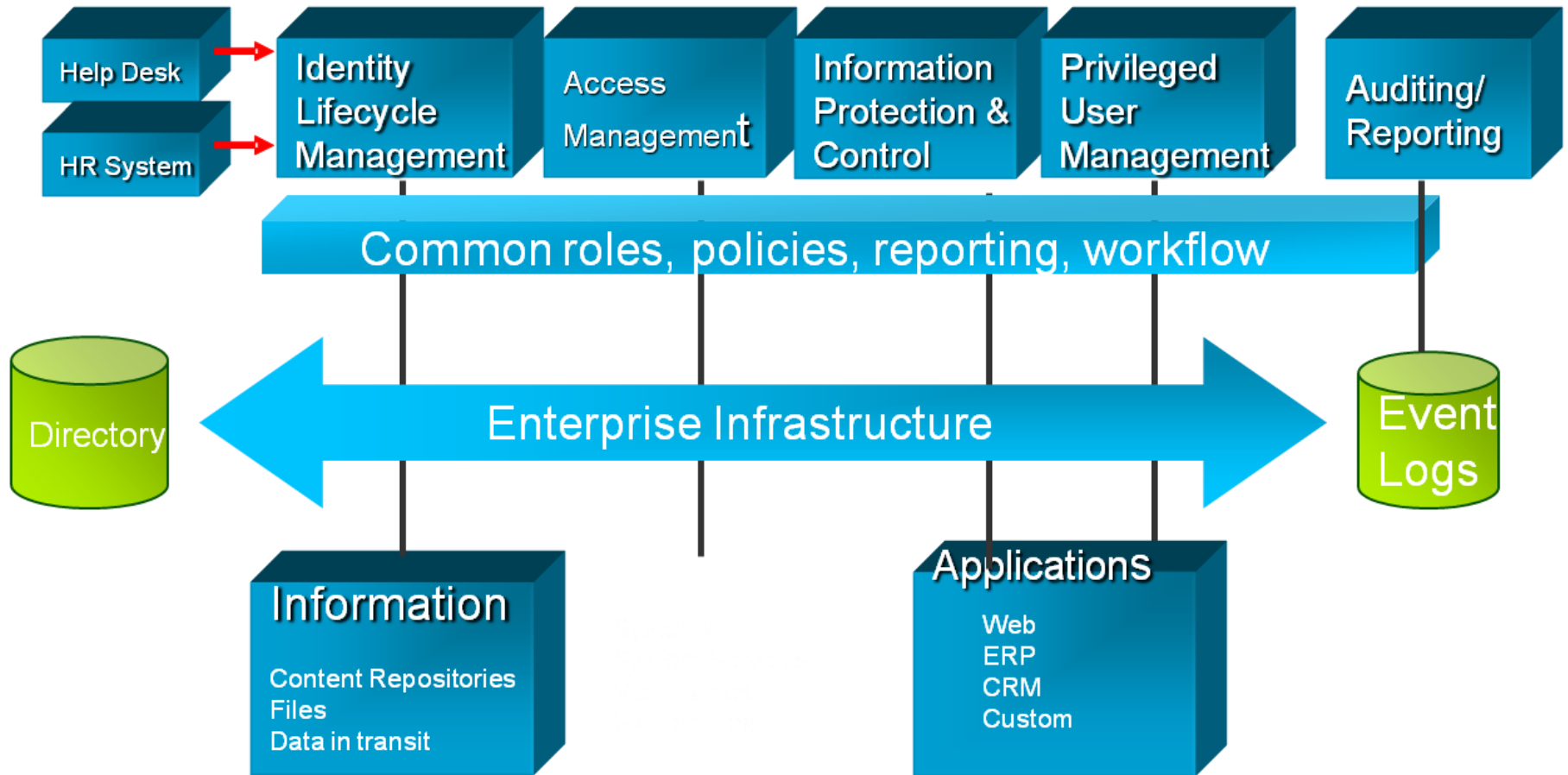


Many Security and Privacy Standards, Technologies

- Fundamental Security Services which support any set of policies
 - Confidentiality, Integrity, Availability
- Huge Inventory of Standards
 - ISO/IEC 27001/2:2005
 - SAML 2.0
 - NIST FIPS 140-2 (crypto modules), FIPS-197 (AES), Special Publications
 - Payment Card Industry-DSS ...
- Mature and Evolving Discipline – Cryptography, IAM, DLP...
- Many Mechanisms/Technologies/Solutions/Products/Implementations

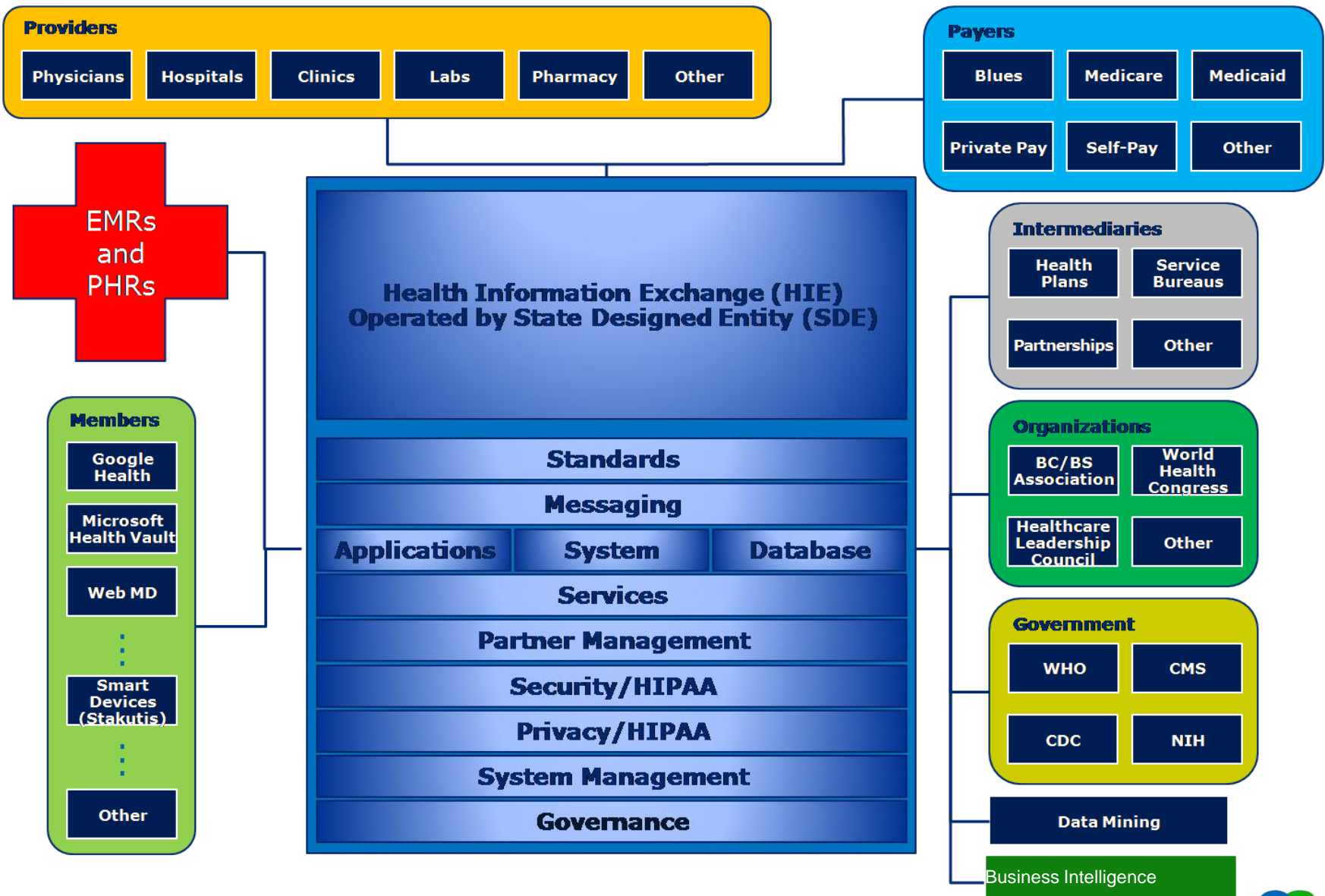
No equivalent body of privacy standards and technologies

...and Compliance/Management Models



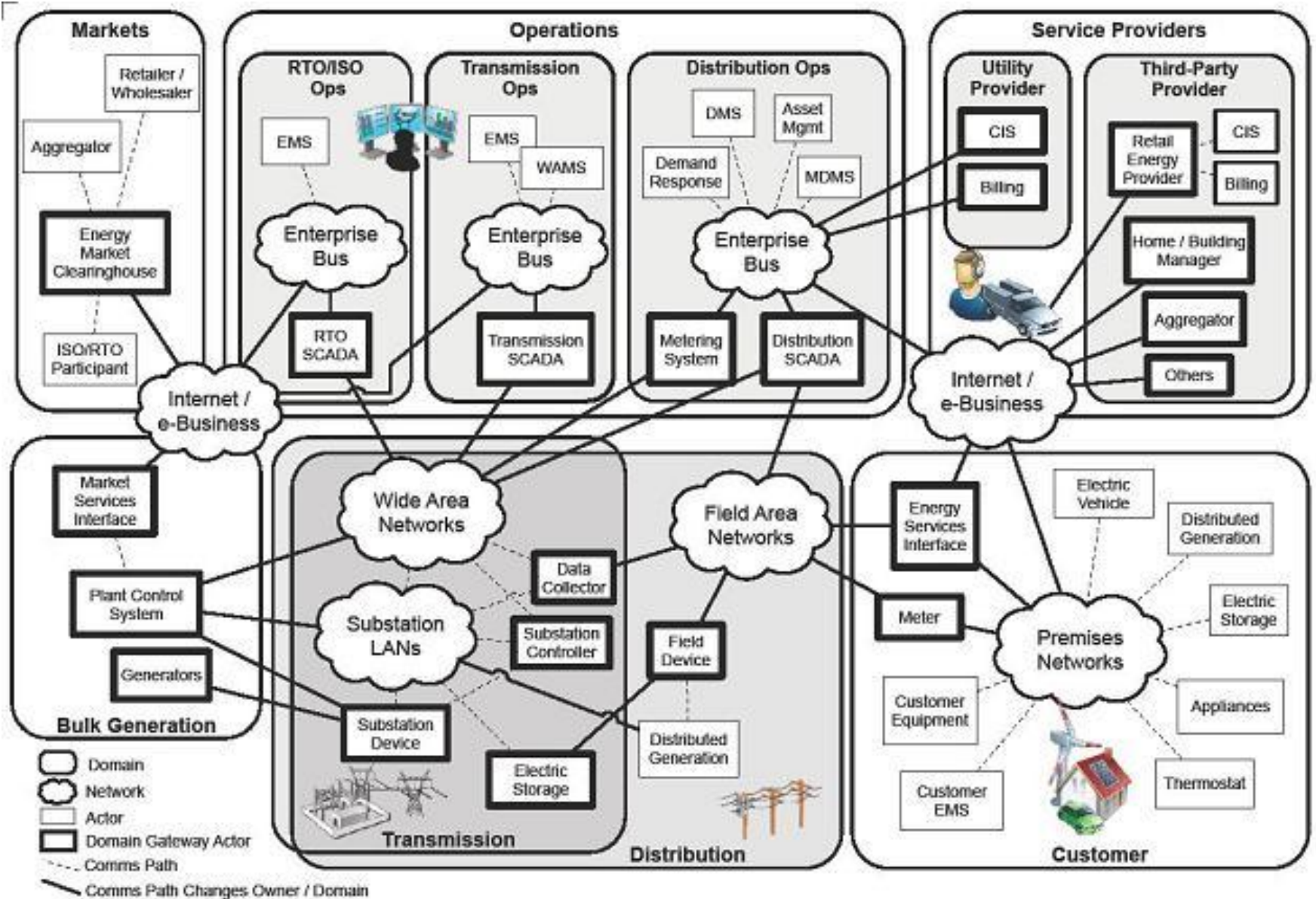
Privacy Management Challenges:

Networked Health IT



Privacy Management Challenges:

Smart Grid



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

NIST Smart Grid Report and Privacy

- 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 included in Chapter 2
- 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

Volumes 2 -3 – NISTIR 7628

— Volume 3 – Supportive Analyses and References

— **Volume 2 – Privacy and the Smart Grid**

- **Chapter 5 – Privacy and the Smart Grid includes**
 - a 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 C – State Laws – Smart Grid and Electricity Delivery
 - 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)

Novel Smart Grid Risk Exposures

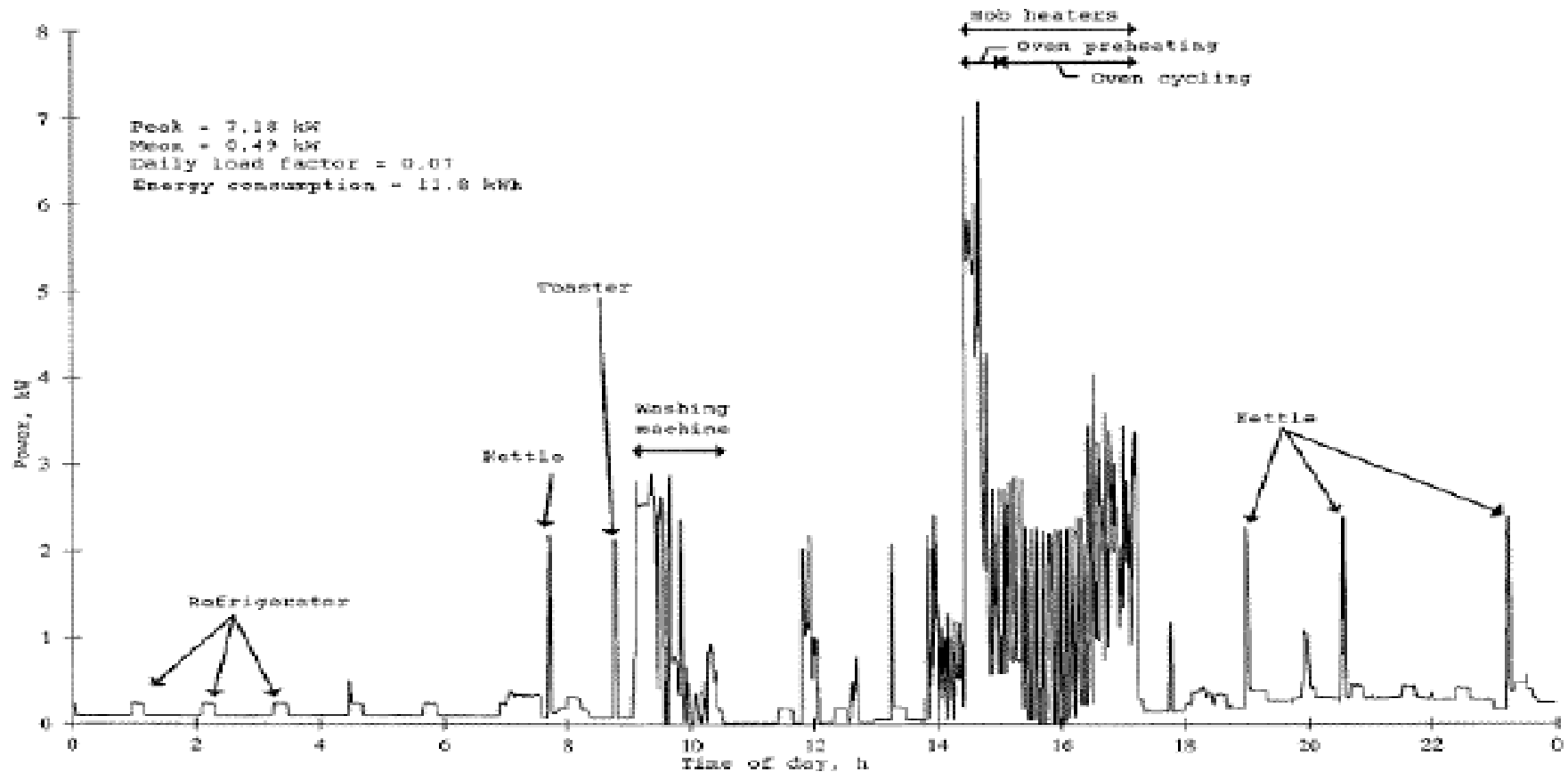


Figure 5-1 Power Usage to Personal Activity Mapping ³⁰

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

What is Missing from the Analysis?

- NISTR 7628 addresses residential users and their data
 - Heavy 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 is a detailed 289-page, report with extensive reference to smart grid architectures and technical security standards

What is Needed?

— Operational Model

- information privacy is the assured, proper, and consistent collection, minimization, processing, communication, use and disposition of personal information (PI) throughout its life cycle
- consistent with data protection principles, policy requirements, and the preferences of the individual

— Lifecycle Model

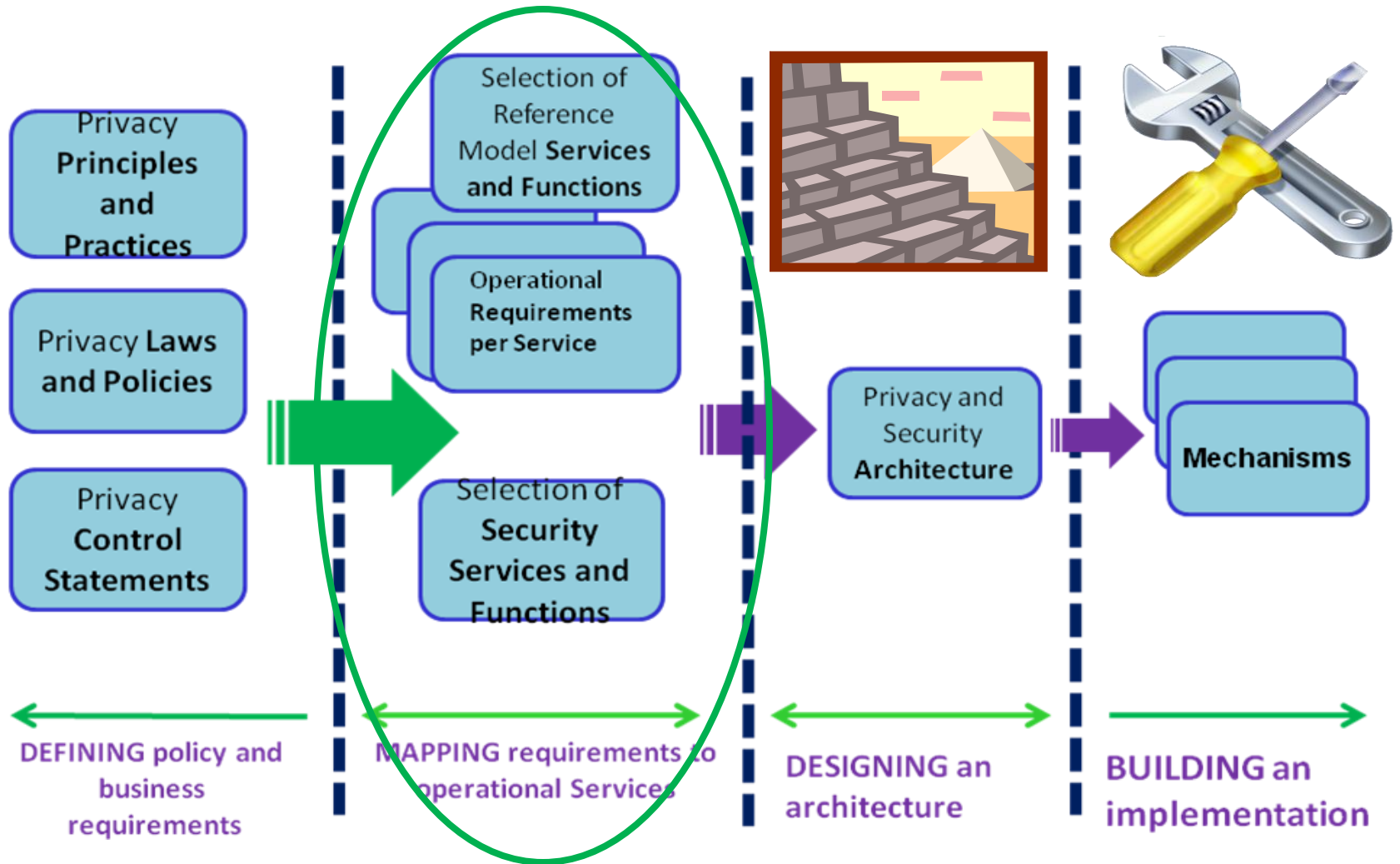
- *Proper* and *consistent* apply throughout the PI life cycle
- apply to all actors, systems, and networks that “touch” the information

*Need an abstract model enabling
full lifecycle privacy management*

OASIS Privacy Management Reference Model (PMRM) Technical Committee

- OASIS PMRM TC formally announced June 27 – first meeting September 8
- complementary to other standards initiatives
- open to all OASIS members
- ISTPA contributed PMRM v2.0 to the TC
- Deliverables
 - the Reference Model
 - one or more use cases utilizing the PMRM
 - 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
 - one or more formal methodologies for expressing use cases

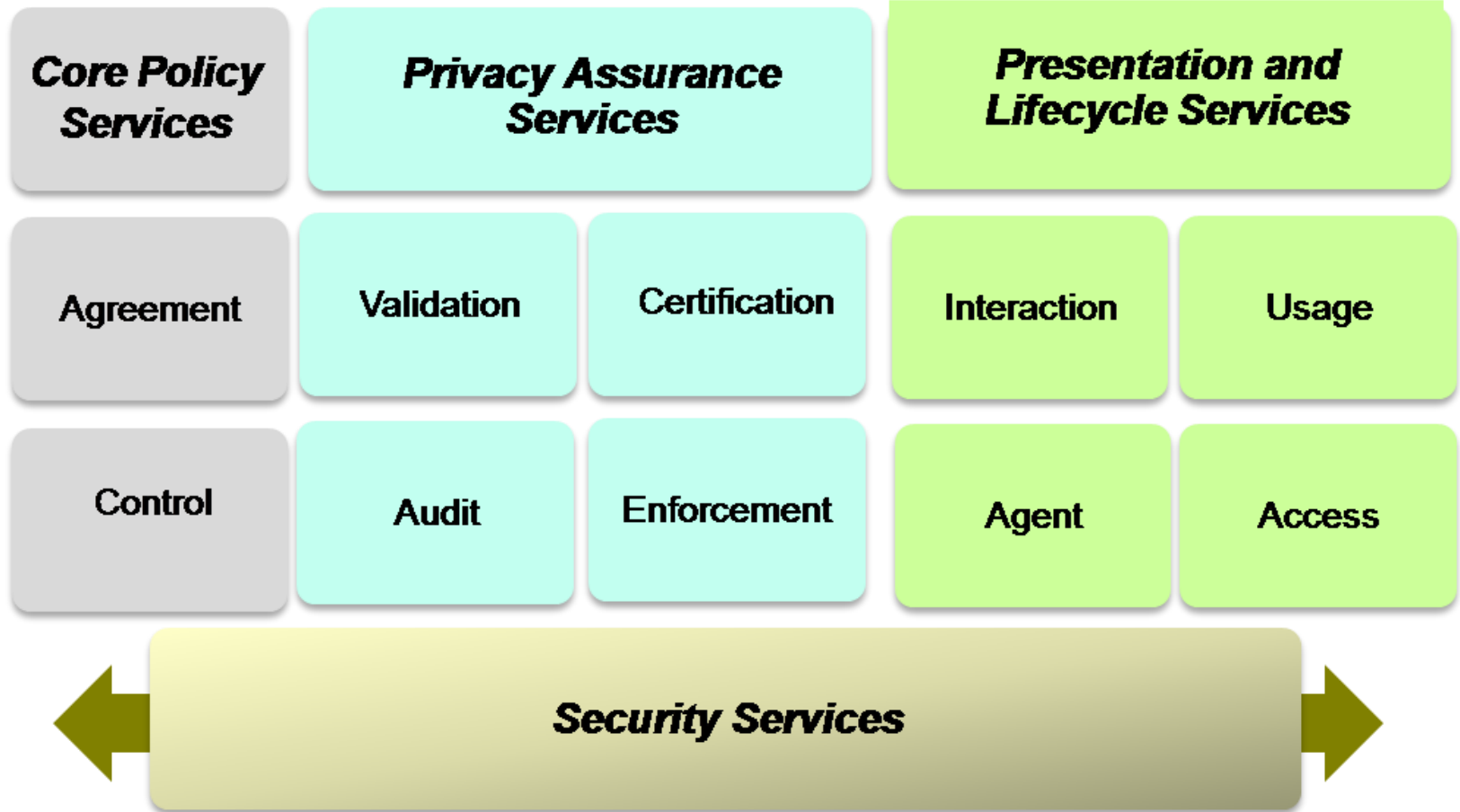
Where Does the Reference Model Fit?



Privacy Management Reference Model – Key Components

- Introductory/explanatory information and motivation
- 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

Privacy Reference Model



Privacy Management Reference Model Services

— Core Policy Services

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

— Presentation and Lifecycle Services

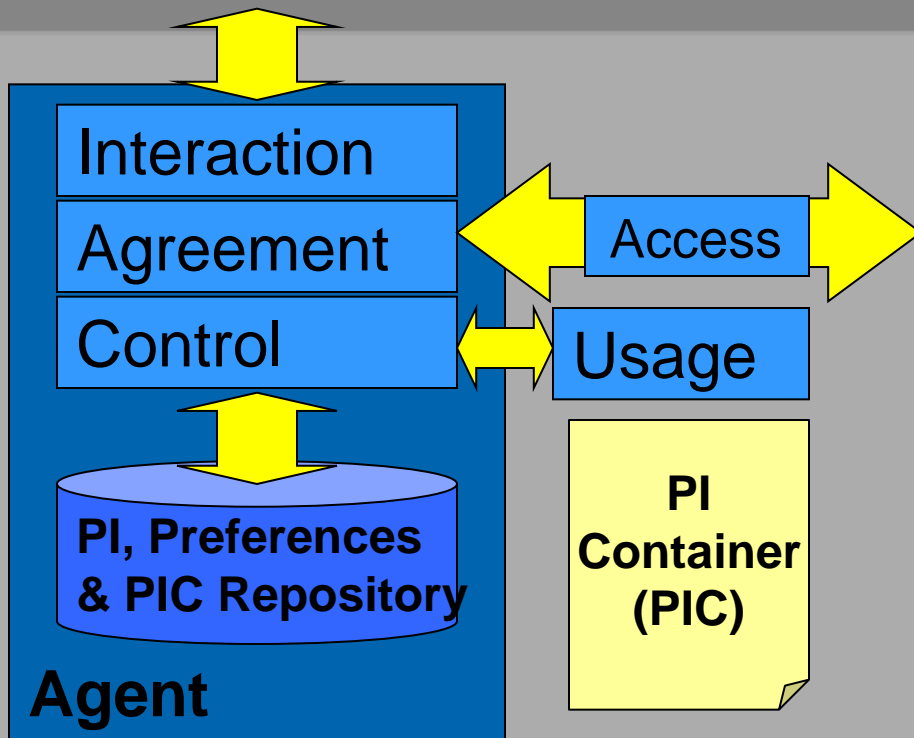
- **Interaction** - manages data/preferences/notice
- **Agent** - software that carries out processes
- **Usage** - lifecycle data use, aggregation, anonymity
- **Access** - individual review/updates to PI

— Privacy Assurance Services

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

"Touch Point" Concept

PI Touch Point



- Each Touch Point node configured with operational stack

- Privacy Policy is an input "parameter" to Control

- Agent is the Touch Point programming persona

-PIC contains PI and usage agreements

Assurance Services

Validation

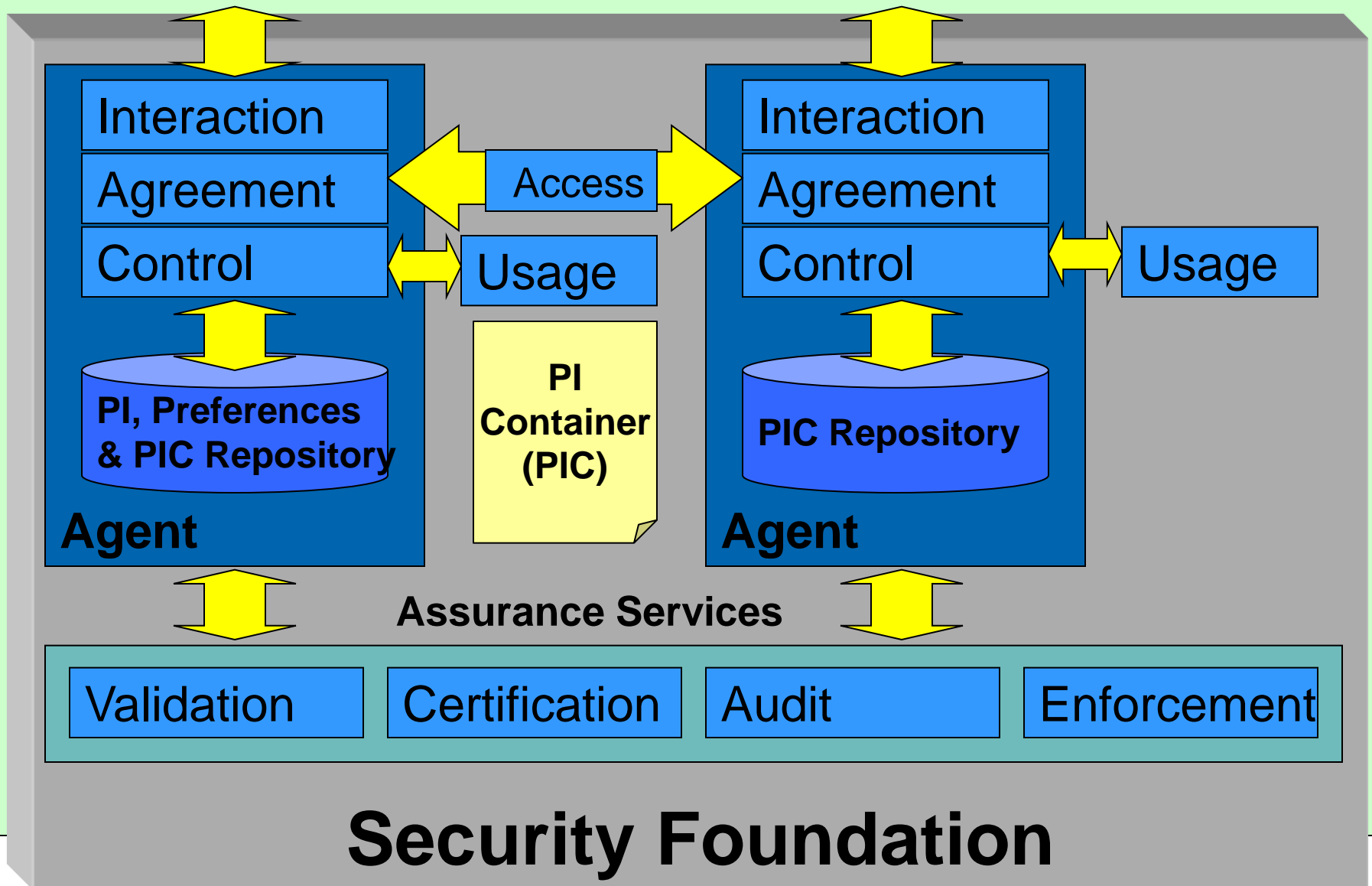
Certification

Audit

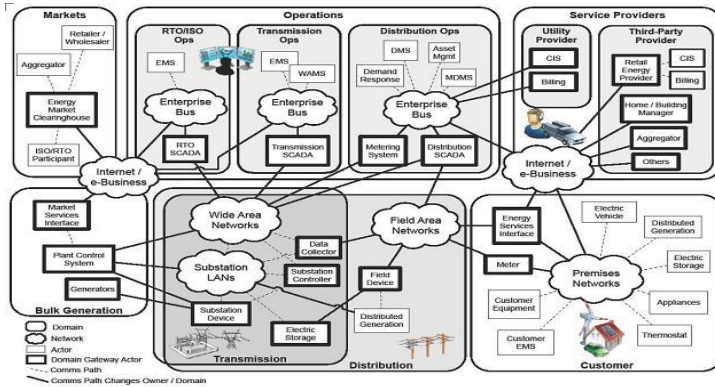
Enforcement

Security Foundation

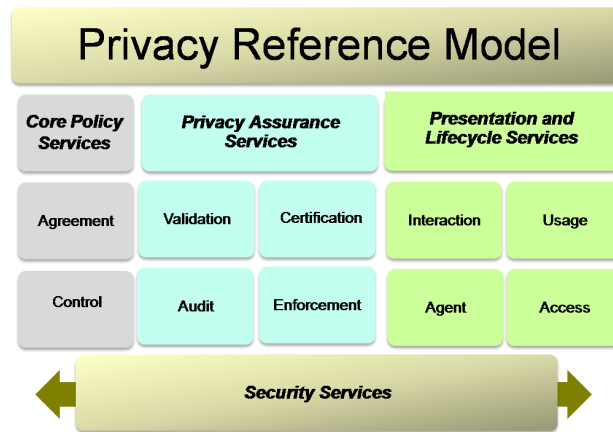
Any two touch points in the PI life cycle



Using the Privacy Management Reference Model

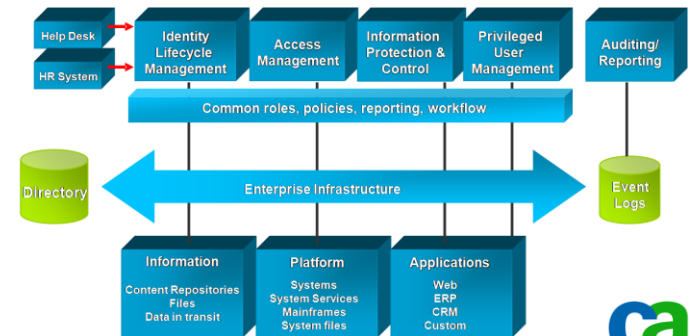


Define privacy requirements for a particular environment-use case



Apply PMRM

Integrate Security Framework



Thank you

John.t.sabo@ca.com

www.oasis-open.org

www.ca.com/cloud