Embedded Java & Secure Element for high security in IoT systems

JavaOne - September 2014

Anne-Laure SIXOU - ST
Thierry BOUSQUET - ST
Frédéric VAUTE - Oracle

life.augmented

ORACLE

Speakers

Anne-Laure SIXOU
Smartgrid Product Line Manager, ST
Anne-laure.sixou@st.com

Thierry BOUSQUET
Smartgrid Application Leader, ST
Thierry.bousquet@st.com

Frédéric Vaute
Master Principal Sales Consultant, Oracle
Frederic.vaute@oracle.com

life.augmented

ORACLE

Session objectives

What is security in IoT systems?

How to combine
Embedded Java and a Secure Element
to secure an IoT system?

life.augmented

ORACLE

Real-world Consumer IoT security today …

Welcome to the "Internet of Things," where even lights aren't hacker safe

Malware attacks on Internet-connected Philips Hue lights cause blackouts.

by **Dan Goodin** - Aug 14 2013, 1:25am +0200

HACKI

Your Home Appliances May be Spying on You

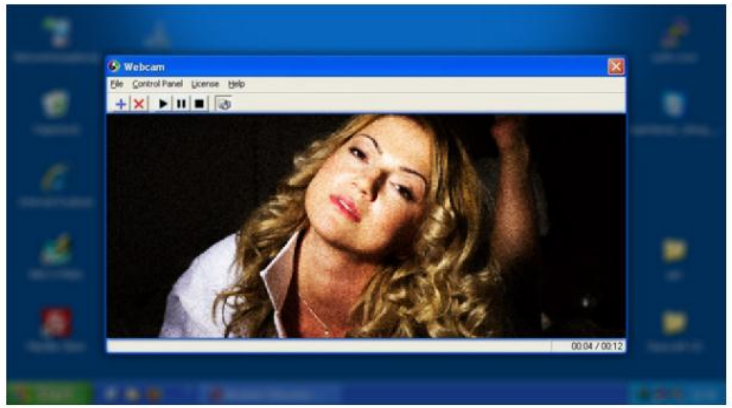
By *Kate Rogers* / *Published August 15, 2013* / *FOXBusiness*

Meet the men who spy on women through their webcams

The Remote Administration Tool is the revolver of the Internet's Wild West.

by **Nate Anderson** - Mar 11 2013, 1:30am +0100

HACKING INTERNET CRIME 232



Control panel backdoor found in D-Link home routers

D-secret is D-logon string allowing access to everything

By Richard Chirgwin, 13th October 2013 Follow 2,018 followers

Smart Meters

Smart meters are a "time bomb" for utilities, warns insurance expert

Jul 23, 2014 Talk Back Free Alerts More On This Topic SHARE

Quick Take: *As an industry, we've done a lot of thinking about the smart meter cost/benefit equation. But I wonder if we've adequately considered what would happen if smart meters made insurance rates go up? Two recent articles in the Insurance Journal suggest that the insurance industry is waking up to this new concern. –* ***Jesse Berst***

Cyber attacks on infrastructure have become a major worry for utilities, warns a **recent article in the Insurance Journal**. Traditionally, energy utilities have kept the grid safe by keeping it separate from the open Internet. But that is rapidly changing as smart meters connect customers to their utilities through the web.

Utilities claim customers have little to fear since those meters will use the same security measures as online banking. But "the risk is being underestimated outside of the industry," said Eberhard Oehler, managing director of German utility Stadtwerke Ettlingen. A recent simulated attack came close to shutting down power to Ettlingen's 40,000 residents. The experiment revealed that "sensitive, critical infrastructure is not sufficiently protected."

life.augmented

ORACLE

Shows the importance of proper security analysis & practical pitfalls …

KERKEY & Embedded Java SE for SmartGrid
a “pre-industrial” tool for players

KERKEY

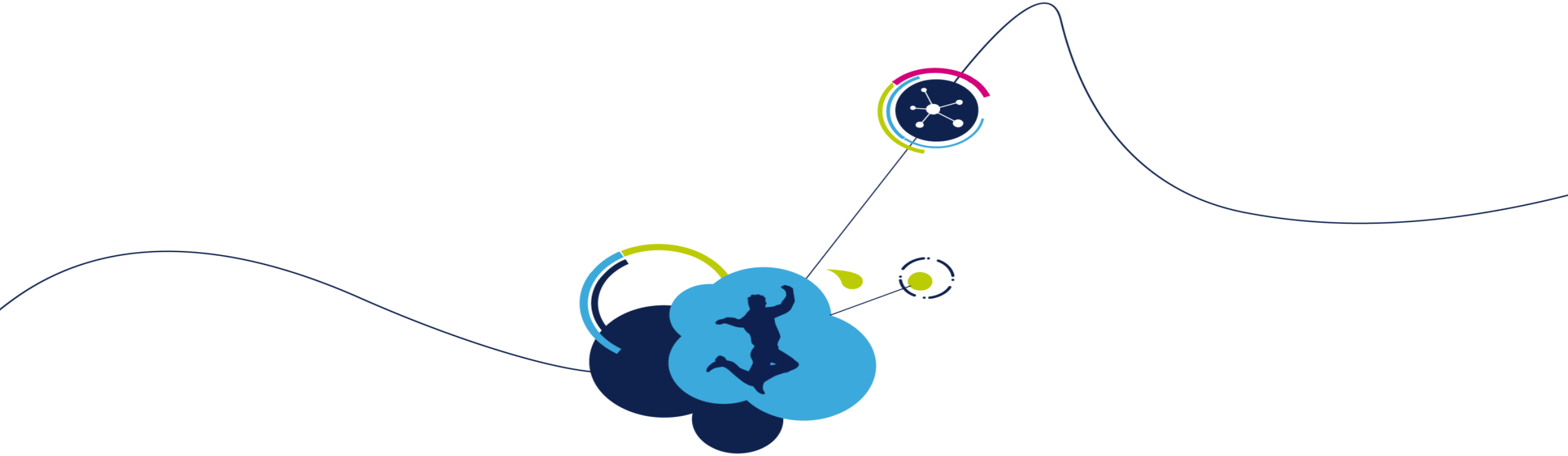
- Highly secure solution certified CC EAL4+
- Flexible solution Java OS and JavaCard application
- Turnkey solution with Industrialization services

Compliant with European & BSI smart metering requirements

Host Embedded Java SE

- Portability on any operating system running on standard desktop system
- High performance system
- Reliable development platform highly deployed

Video : Secure Smartgrid solution



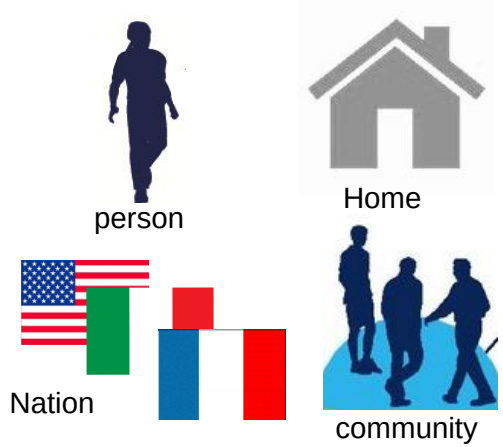
General security concepts

life.augmented

ORACLE

Why security is important ?

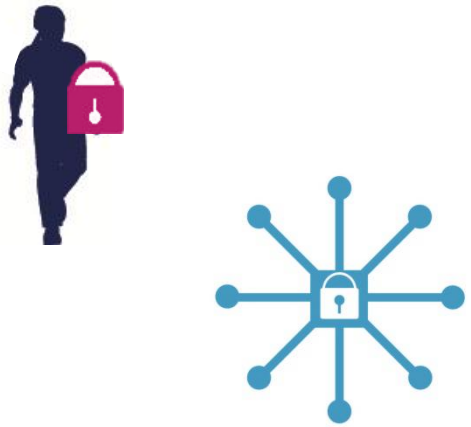
Security is the degree of resistance to, or protection from, harm. It applies to all vulnerable and valuable assets such as :



There are two reasons why security should be an important item for everyone :

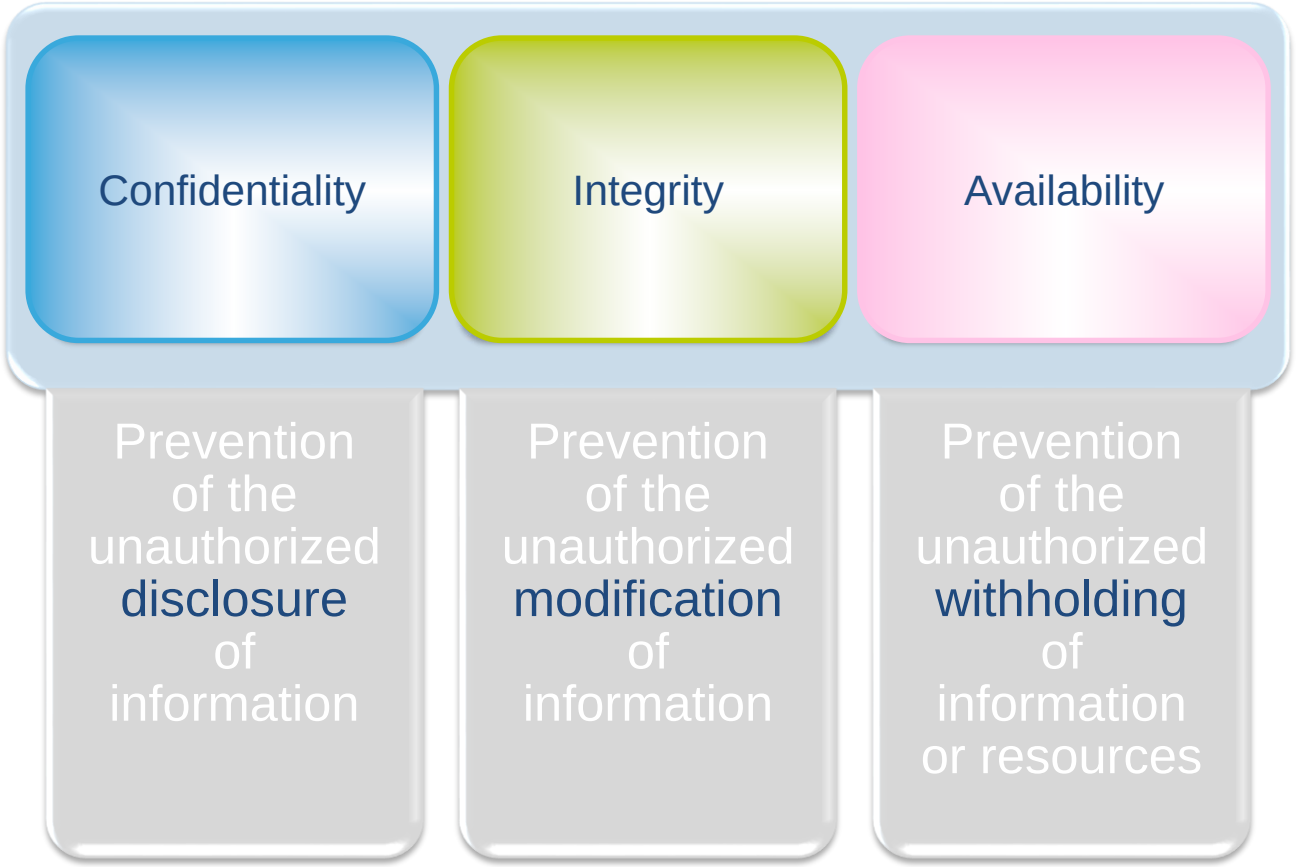
Personal Protection of Information

Social Responsibility
To protect the group you join when you connect your machine to the network



Information Technology Security

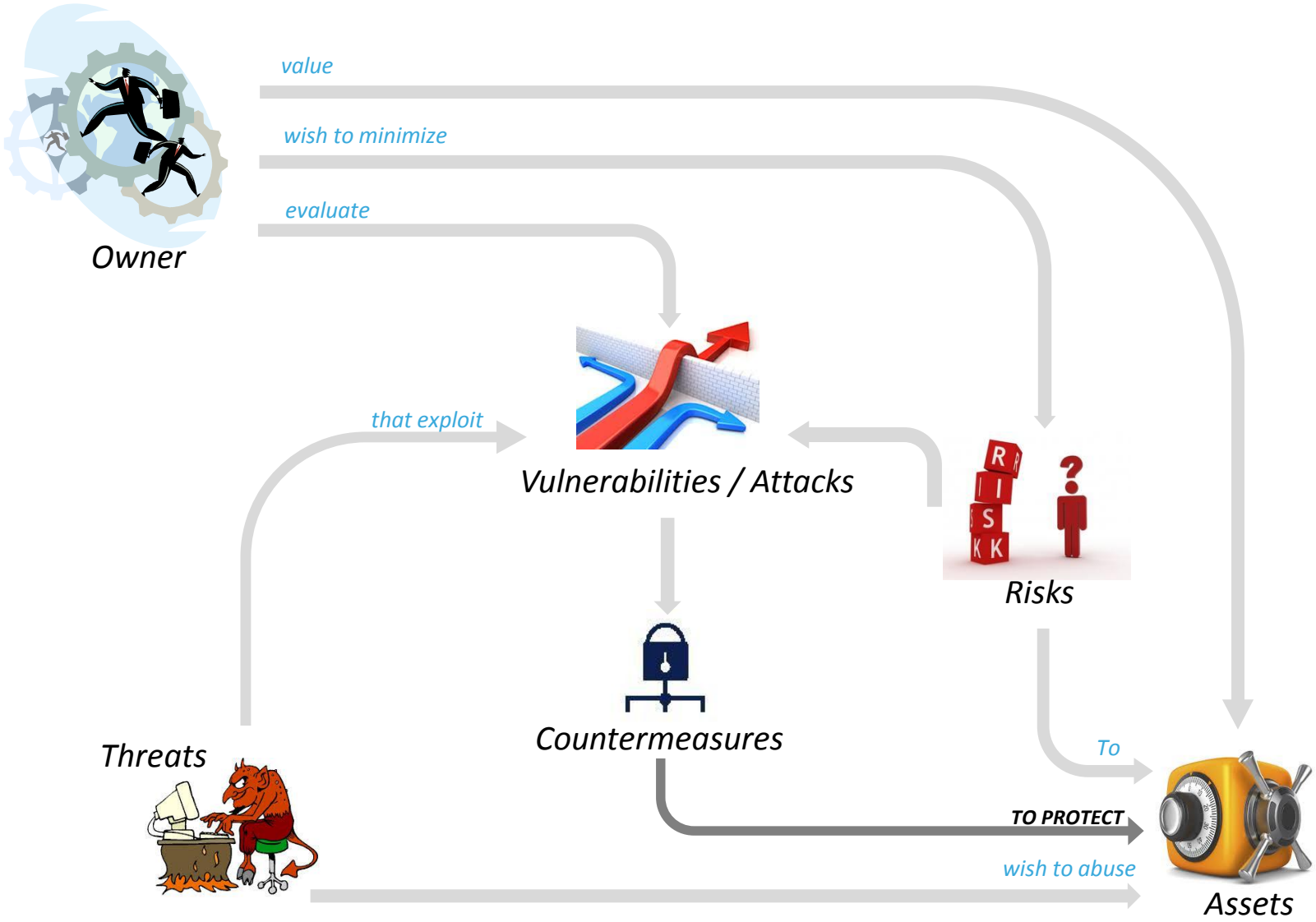
main prevention of information



Individuals or companies expect that their personal information contained in IoT products or systems

- Remains private
- Not to be subjected to unauthorized modification
- Be available to them

Security concepts and relationships



Designing secure systems

- Infrastructure and set of rules
- Components
  - Secure devices (e.g. Microcontrollers)
    - performing crypto with
    - ... cryptographic keys
    - ... protected logically and physically
  - Software on other platforms
    - offering only limited protection to data and code
  - Central computers: hosts
  - Telecommunication infrastructure
- Set of participants, each with a specific role

  Every party has a set of **rules** he/she should follow

How to combine Embedded Java and a Secure Element to secure an IoT system ?

life.augmented

ORACLE

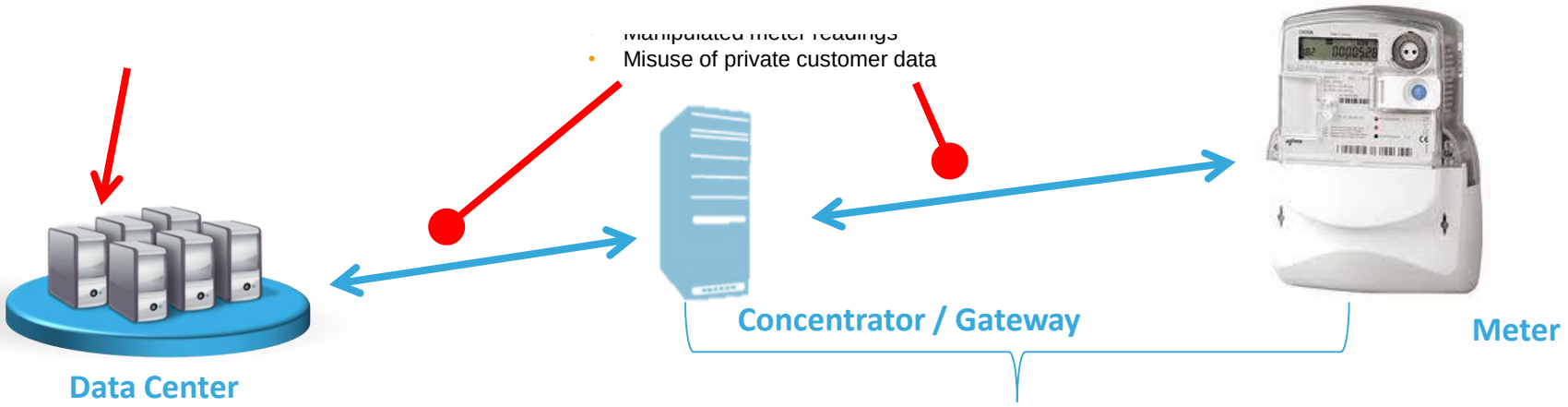
From threats in Smart Metering …

Fake server

- Commercial & cyber crime usage
- Disruption of administration system

Data Collection & Corruption

- Fraud for invoices
- Misuse of private customer data



Fake services

- Supply shut down – Disruption of service
- Spread of wrong information (e.g. invoices)
- Distributed denial-of-service
- Malicious code

Fake server / device

- Supply shut down
- Supply shut down

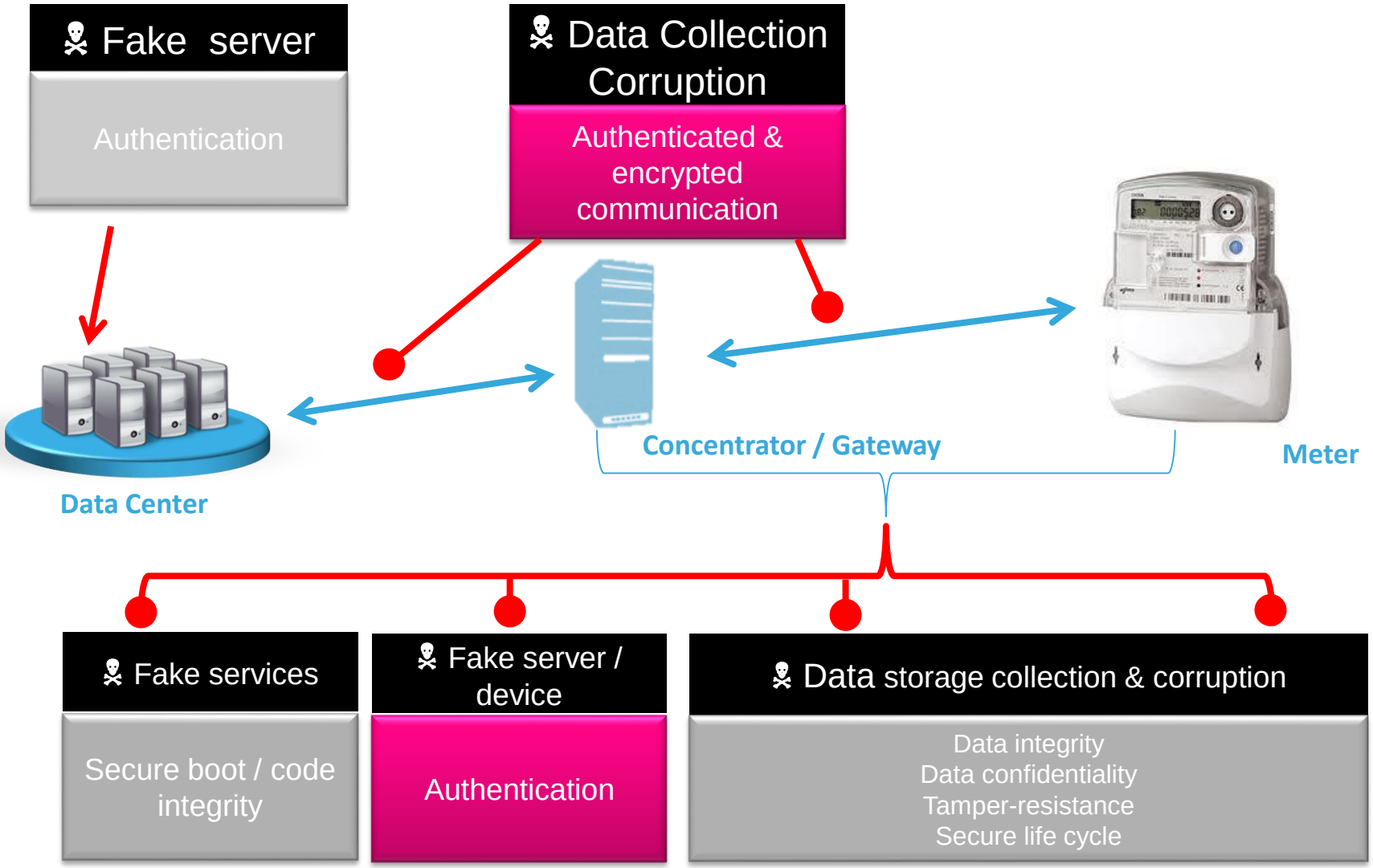
Data storage collection & corruption

- Identified empty houses
- Fraud for invoices
- Manipulated meter readings
- Misuse of private customer data

life.augmented

ORACLE

… to Countermeasures

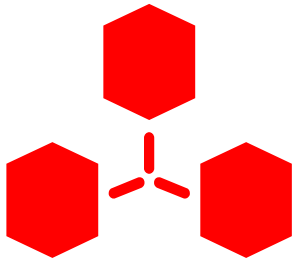


The solution with Java and ST products

Threats	Solution	Implementation & services requested
Fake devices	**Authenticated devices**	**Mutual authentication**
Data collection & corruption	**Authenticated & encrypted communications (secure channel)**	Expertise
		SW Crypto libraries
		HW Crypto accelerators
		Robust implementations
		Network security protocols
		Evaluated / Certified
Fake services	Robust Smart-Devices (secure boot & code integrity)	Authenticated software stacks
		Least privilege, Sand-boxing & Isolation of assets
		Detection & Monitoring
Data storage collection & corruption	Protected crypto keys & private data (data integrity, data confidentiality and tamper-resistance)	From PCB attacks
		From SW attacks
		From sophisticated HW attacks
	Security Provisioning & Life Cycle Management	Provisioning of secrets in ST chips
		Support for sophisticated multi-stakeholders scenarios & field management

IoT requires smarter and more secure devices

Local intelligence and decision-making

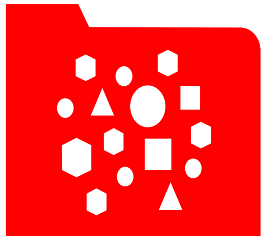


Flexible networking

Performance and scalability

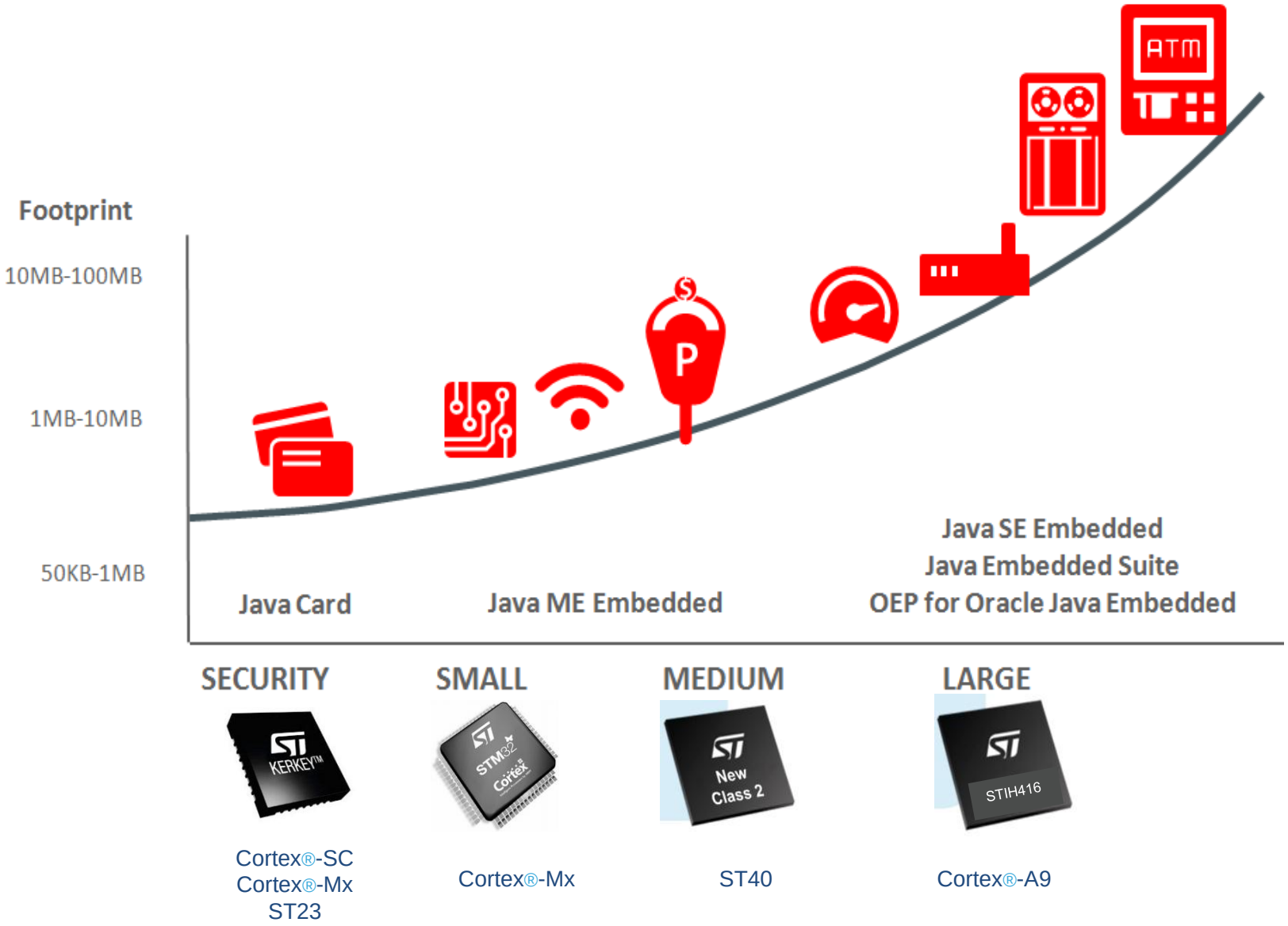
Security

Remote management



Functions become services

Java platforms on ST chipsets



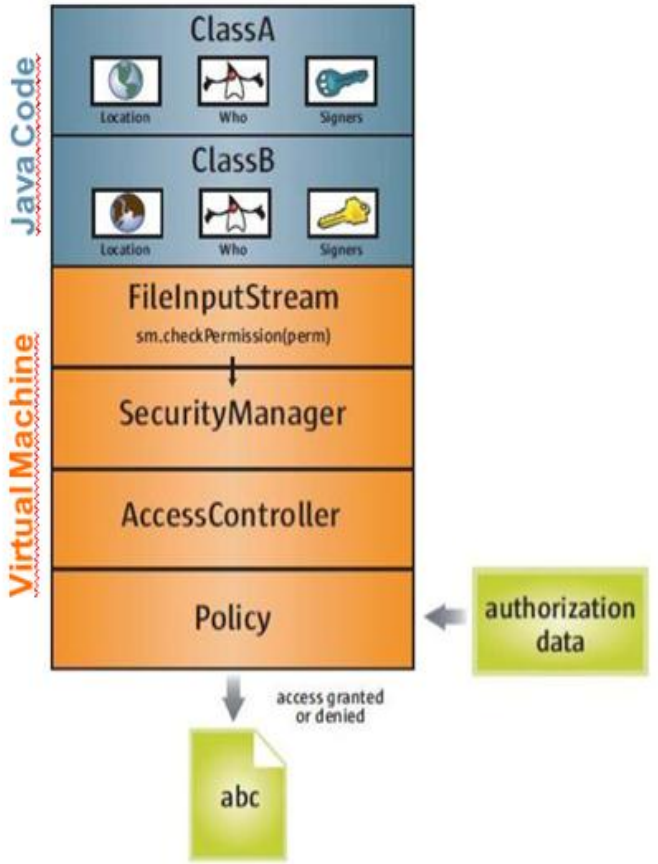
life.augmented

ORACLE

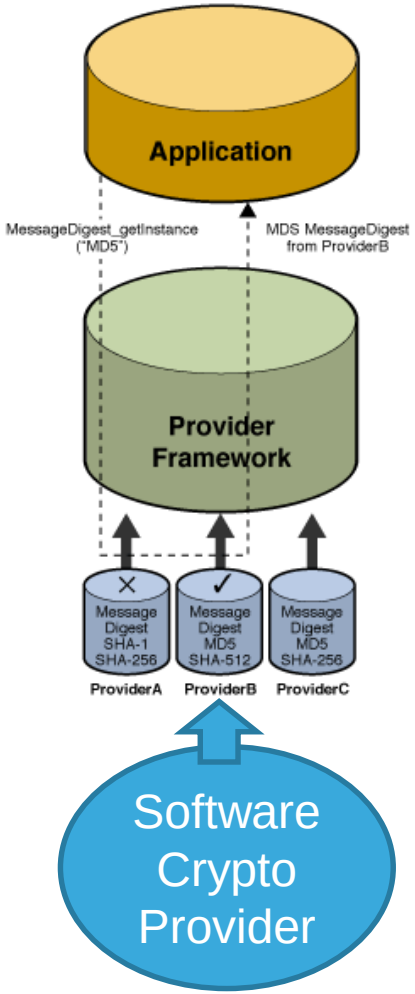
Java SE Security Overview

Secure and controlled code execution

- Runtime security: “Sandbox” Concept
  - Controlled code loading
  - No file access on host, limited network access, no native code execution
- Security Manager / AccessController
  - Limits access to resources and data by means of runtime security
- Security Policy
  - Configurable definition of the limits of the Security Manager (permissions)
- Domains
  - Act as instances of Security Policy
  - Define access for different areas of code through source of the request

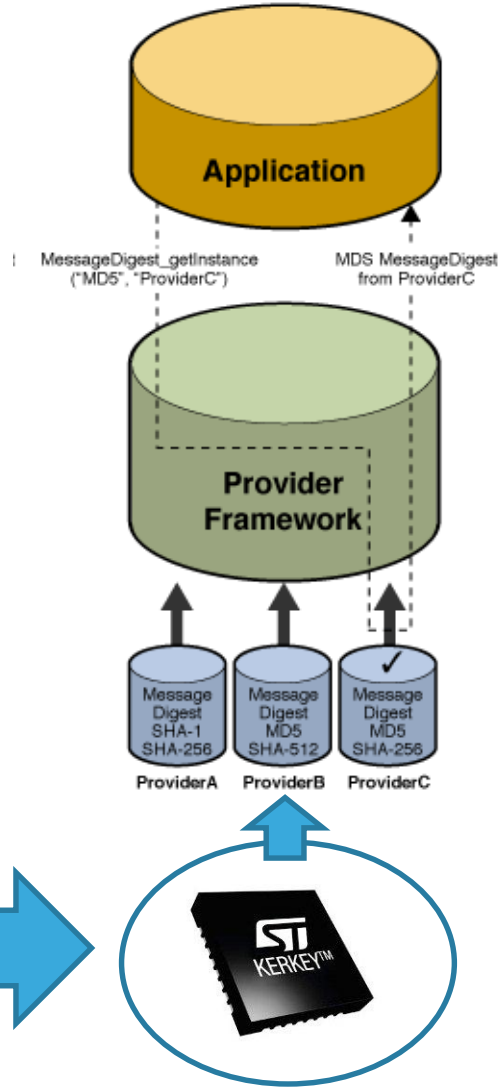


Java SE Cryptography Architecture (JCA)



- JCA (Java Crypto Architecture) Provides an extensible, full featured API for building secure applications
- Algorithm and implementation independent
- Provider-based architecture
  - Allows extension of Java Security to hardware based security with Secure Element

From software to hardware based security



life.augmented

ORACLE

Secure Element Growth Drivers

Secure RF

eSE-NFC

ePROTECT

PERSONAL SECURITY

EMBEDDED SECURITY

SMARTCARD

Contactless platform: ST31

e-Flash flexibility

MOBILE

NFC secure element: ST33

NFC combo: SE + CLF

CONSUMER & INDUTRIAL

End-to-end turn key solutions

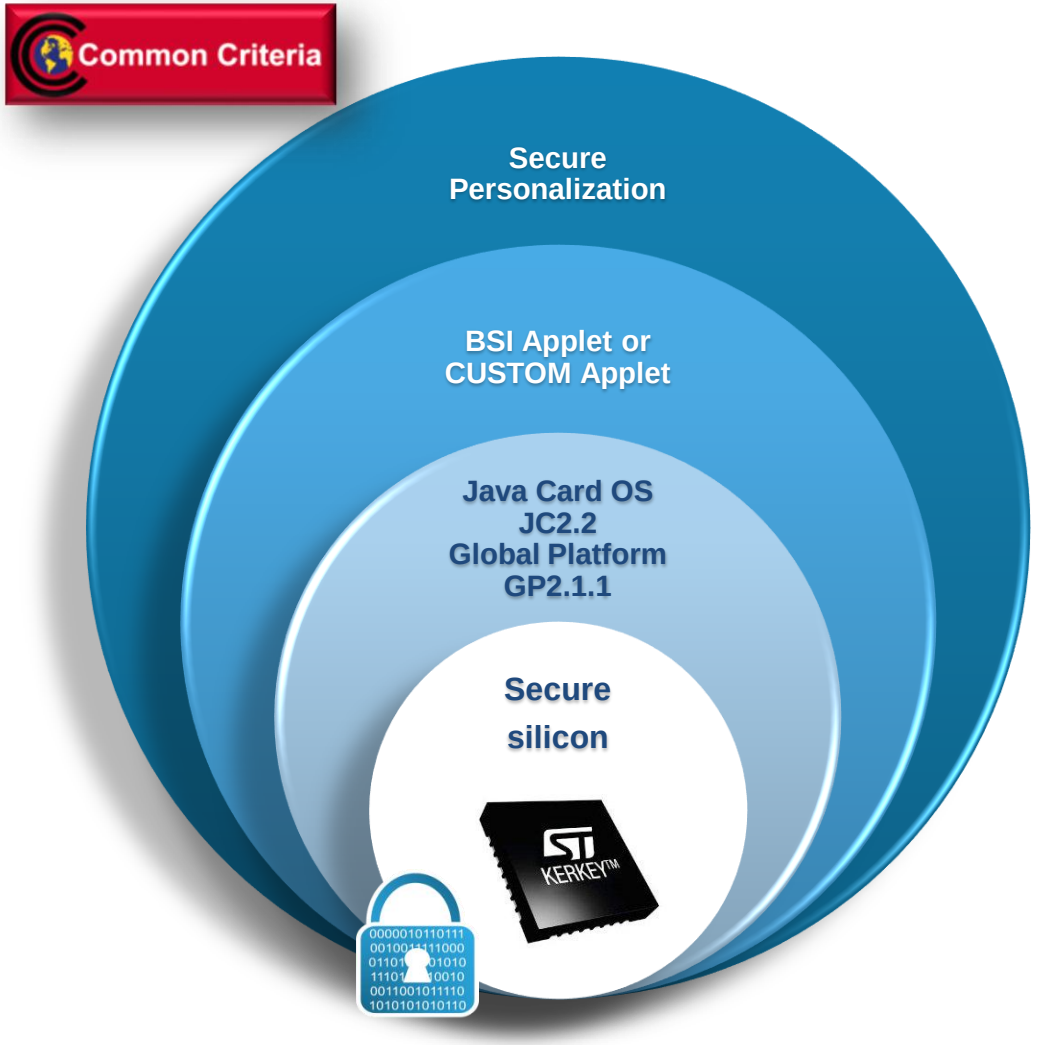
Hardware, Software, Perso

SE=Secure element
CLF = Contact-Less Frontend

life.augmented

ORACLE

KERKEY
Secure element for smartgrid system

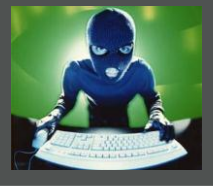
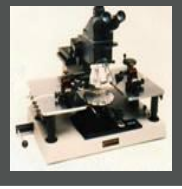
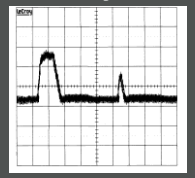
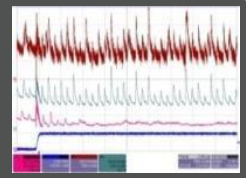


- Highly secure solution certified CC EAL4+ (Hardware – firmware – personalization)
- Java platform with modular Java Card application
- Industrialization & Personalization services
- QFN32 suitable package for Smart metering & Industrial design

life.augmented

ORACLE

Leading edge methodology for Security

Material / IP theft	Physical attacks	Fault injection	Side channel analysis
			
Secure manufacturing and development environments and flows Product life cycle management	Shields Intrusion detectors Obfuscation	Dedicated architecture and design Detectors HW and SW countermeasures	Crypto and product architecture and design Solid crypto SW

Internal & external audits, regular maintenance

Internal assessment : best in class labs and methodology
Silicon technology advanced analysis tools
External Labs assessment - R&D projects, Technology watch

Evaluation and Certification by public authorities, Common Criteria, EMVCO, FIPS …

life.augmented ORACLE FIPS 140-2 CRYPTOGRAPHY FIPS EMVCo Common Criteria

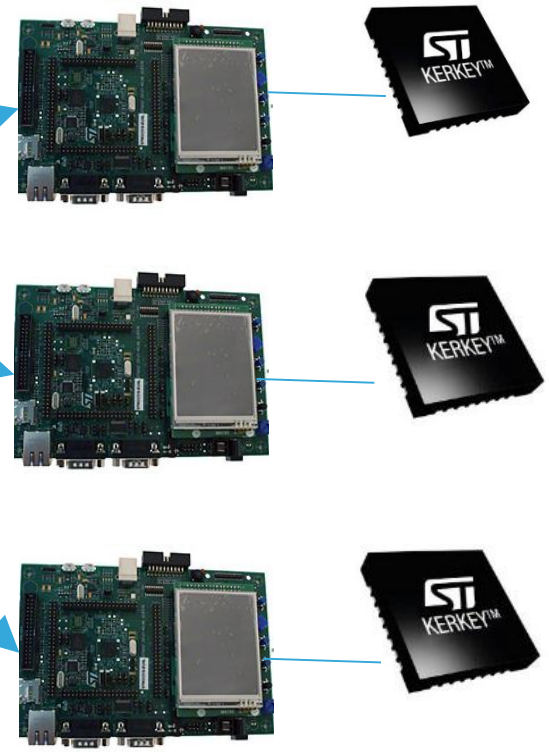
Smartgrid solution architecture

Energy Provider data Center

Concentrators (TLS server)

Secure Smart meters (TLS client)

STIH416 processor : Cortex®-A9
Linux + Java SE Embedded
+
ST Kerkey
Java Card + Global Platform v2



ST STM32 + ST Kerkey
Java Card + Global platform v2

life.augmented

ORACLE

Java

High level Security can be reached if Kerkey is added to Java solution

Threats	Solutions		Java	Kerkey + Java	Kerkey Implementation
Fake Devices	**Authenticated Devices**	**Mutual authentication**	**STD**	**HIGH**	**Java key store is protected inside Kerkey**
Data collection & corruption	**Authenticated & Encrypted Communications (secure channel)**	Expertise	STD	HIGH	AES & SHA-3 inventors are ST employees
		SW Crypto libraries	**STD**	**HIGH**	**New security provider can be added to JCE/JCA to extend cryptographic features with Kerkey**
		HW Crypto accelerators	NA	HIGH	In ST products
		Robust implementations	HIGH	HIGH	Including tamper-resistant Secure uC
		Network security protocols	STD	HIGH	Available for ST products
		Evaluated / Certified	NA	HIGH	Some products, IPs & libraries evaluated by third parties or Common Criteria certified
Fake Services	Robust Smart-Devices (secure boot & code integrity)	Authenticated Software Stacks	STD	HIGH	Secure boot, flash protection & dedicated TPMs Secure Firmware Upgrade & Protected JTAG
		Least privilege, Sand-boxing & Isolation of assets	NA	HIGH	Hardware filters and firewalls, dedicated security subsystems, Trusted Execution Environment, TrustZone technology, dedicated Secure Elements & Secure uC
		Detection & Monitoring	NA	HIGH	Tamper-detection & environmental sensors in some products
Data storage collection & corruption	Protected Crypto Keys & private data	From PCB attacks	NA	HIGH	On-chip storage with eNVM scrambled and encrypted, HW secure protection
		From SW attacks	NA	HIGH	Hardware filters and firewalls, dedicated security subsystems, Trusted Execution Environment, TrustZone technology, dedicated Secure Elements & Secure uC
		From sophisticated HW attacks	NA	HIGH	Tamper-resistant & third-party evaluated security subsystems Dedicated, tamper-resistant and CC-certified Secure uC
	Security Provisioning & Life Cycle Mgt	Secrets provisioning in ST chips	NA	HIGH	Programming of crypto keys by ST at manufacturing Secure Manufacturing Environment
		Support for sophisticated multi-stakeholders scenarios & field management	NA	HIGH	Global Platform Compliant • Tamper-resistant Secure Element (SE) and secure SW for SoCs • Trusted Execution Environment (TEE) for SoCs

life.augmented

ORACLE

Exemple of high level security Java solution with Kerkey

Threats	Solutions	Java	Kerkey + Java	Kerkey Implementation
Fake Devices	Mutual authentication	STD	HIGH	Java key store is protected inside Kerkey
Data collection & corruption	SW Crypto libraries	STD	HIGH	New security provider can be added to JCE/JCA to extend cryptographic features With Kerkey

Typical Software architecture

Meter MCU or Concentrator MPU

Java application

JCE/JCA

SUN PKCS#11 Provider

Java SE or ME

ST PKCS11 Middleware

Operating system

Secure element Kerkey

Java Card application : smart metering

Java Card 2.2 GP 2.1.1

Operating system

Serial link
ISO7816 or I2C

life.augmented

ORACLE

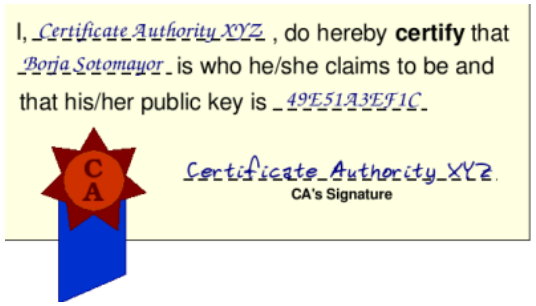
Demo for developpers

Demo usage of Kerkey secure element with Java SE & Java card

- Demo 1 : Open a secure session from Java

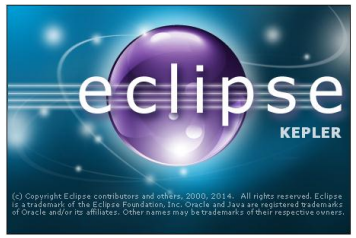
  Read CPLC data's are often used to identify the chip in the field

- Demo 2 : Generation of certificate signature request using Kerkey



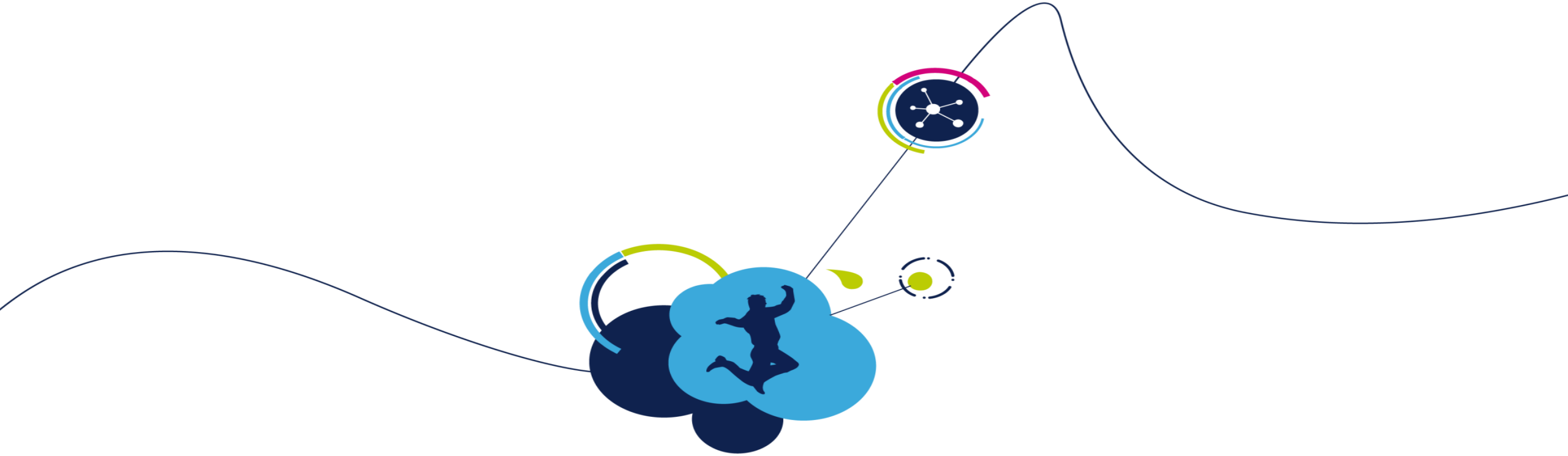
- A certificate is an electronic document used to prove ownership of a public key
- It allows to authenticate documents, open secure channel SSL, etc ,,,
- Certificate signature request is one part of the creation of the certificate
- It allows newly generated signature to be signed by Certificate Authorities.

Demo using :



life.augmented

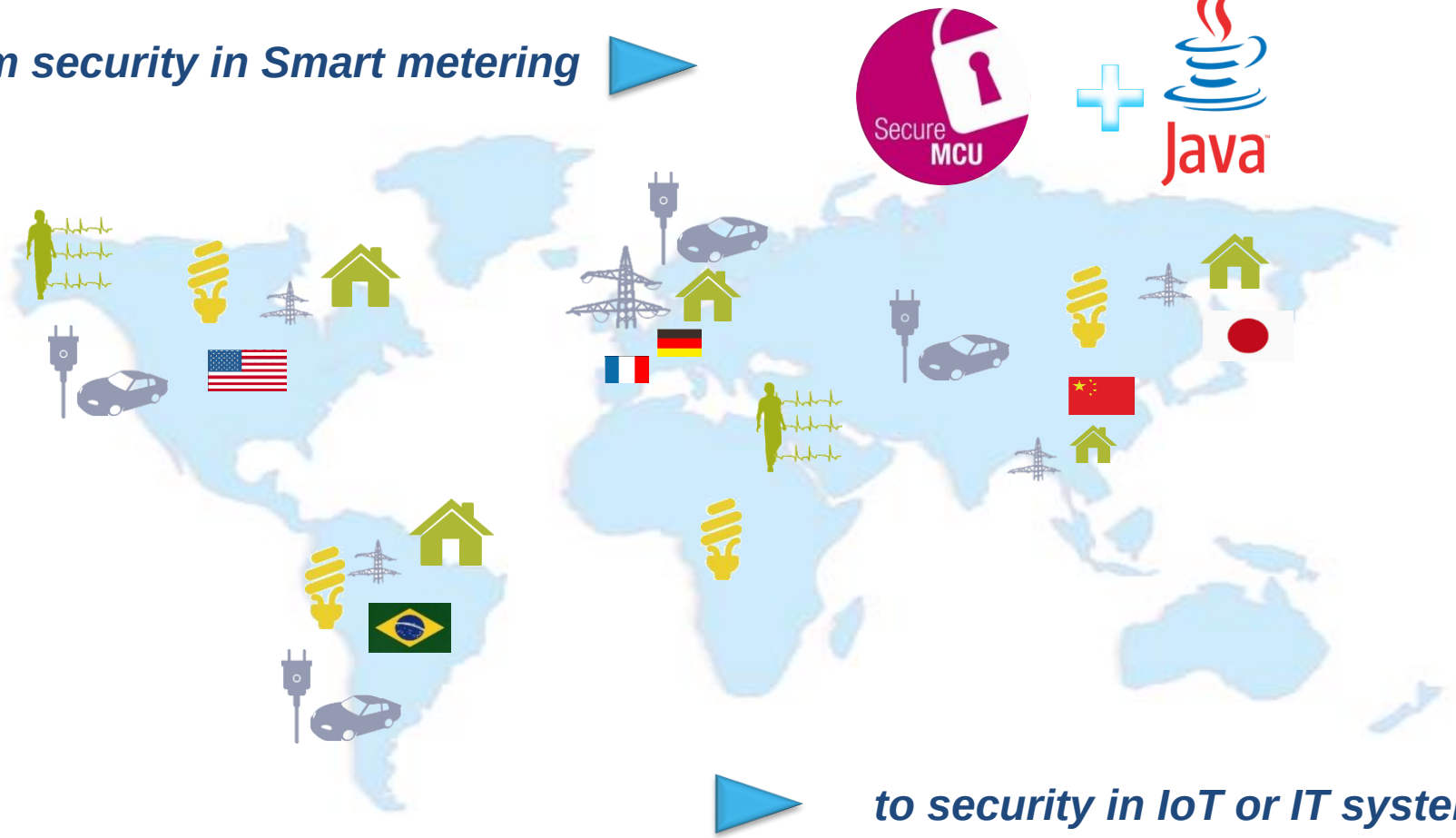
ORACLE



Conclusion

and the future…

From security in Smart metering



to security in IoT or IT systems

For more information of how to address Smart Home system, visit

"Universal Development Kit for Creating and Deploying Smart Home/Building Applications [CON2405] session"

life.augmented

ORACLE

Contacts

- Join ST people
  - USA : Serge.fruhauf@st.com
  - APAC : Bruno.batut@st.com
  - EMEA : Fabrice.gendreau@st.com
  - Japan / Korea : Michel.faure@st.com

- www.st.com / kerkey

TUESDAY, SEP 30, 2014

Conference Sessions

Universal Development Kit for Creating and Deploying Smart Home/Building Applications Fred Vaute, Master Principal Sales Consultant, Oracle Luca Celetto, Stmicroelectronics (north America) Holding, Inc. Oleg Logvinov, Director, Special Assignments, STMicroelectronics	11:00 - 12:00	Hilton - Continental Ballroom 1/2/3	CON2405

life.augmented

ORACLE