

GlobalPlatform technology for the web

How browsers may benefit from GlobalPlatform TEE and SE

to offer secure and convenient services

Hervé Sibert
System security architect, Director, STMicroelectronics
Chair of GlobalPlatform TEE Security WG

W3C WebCrypto.Next workshop
September 10-11, 2014

@GlobalPlatform_

www.linkedin.com/company/globalplatform

GlobalPlatform Positioning

GLOBALPLATFORM™

GlobalPlatform is ***the*** standard for managing applications on secure chip technology

TRUSTED EXECUTION ENVIRONMENT

MESSAGING

SECURE ELEMENT

Across several market sectors and in converging sectors

PREMIUM CONTENT | FINANCIAL | TELECOM | GOVERNMENT | AUTOMOTIVE | HEALTHCARE | RETAIL | TRANSIT

GlobalPlatform technologies

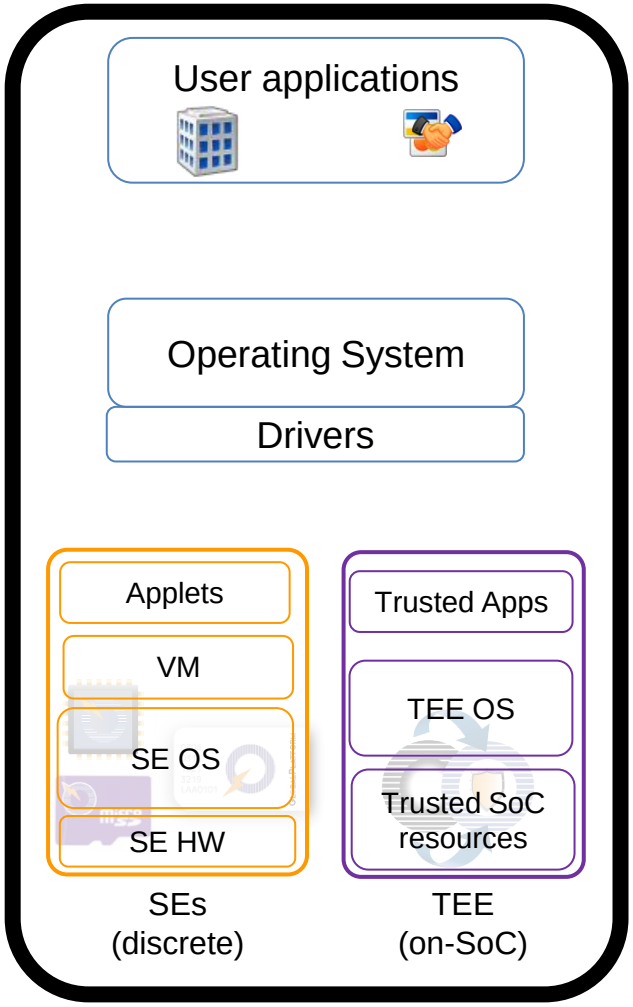
- Management of applications from multiple stakeholders on
  - Secure Element
  - Trusted Execution Environment (TEE)
- APIs specification for app development in TEE/SE
- Qualification processes
  - Interoperability
  - Security

SE/TEE head-end

GlobalPlatform technologies

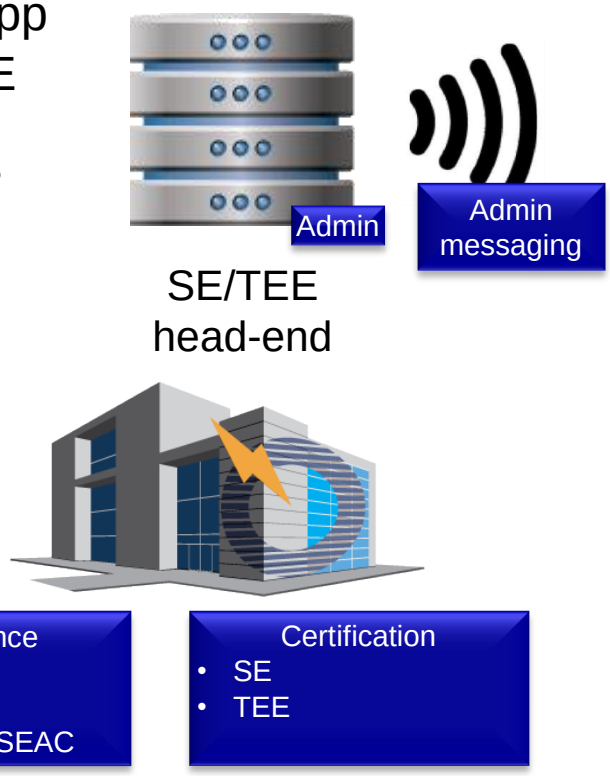
- Management of applications from multiple stakeholders on
  - Secure Element
  - Trusted Execution Environment (TEE)
- APIs specification for app development in TEE/SE
- Qualification processes
  - Interoperability
  - Security

SE/TEE head-end



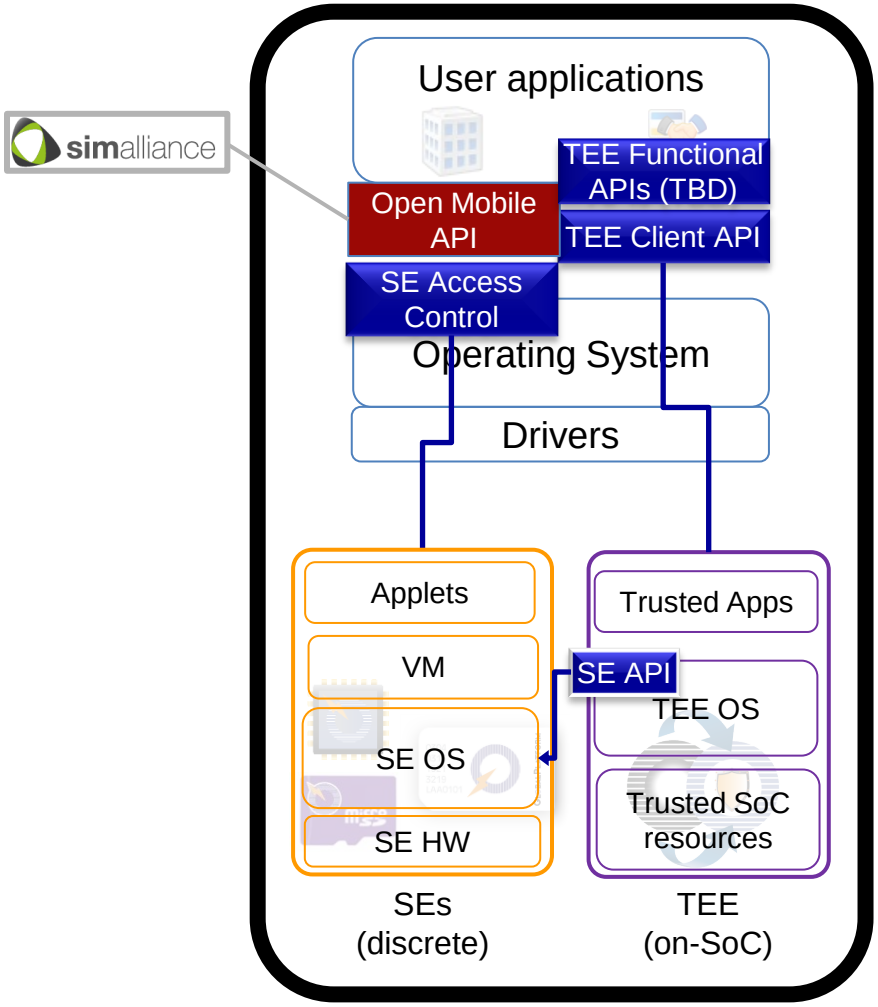
GlobalPlatform technologies

- Management of applications from multiple stakeholders on
  - Secure Element
  - Trusted Execution Environment (TEE)
- APIs specification for app development in TEE/SE
- Qualification processes
  - Interoperability
  - Security



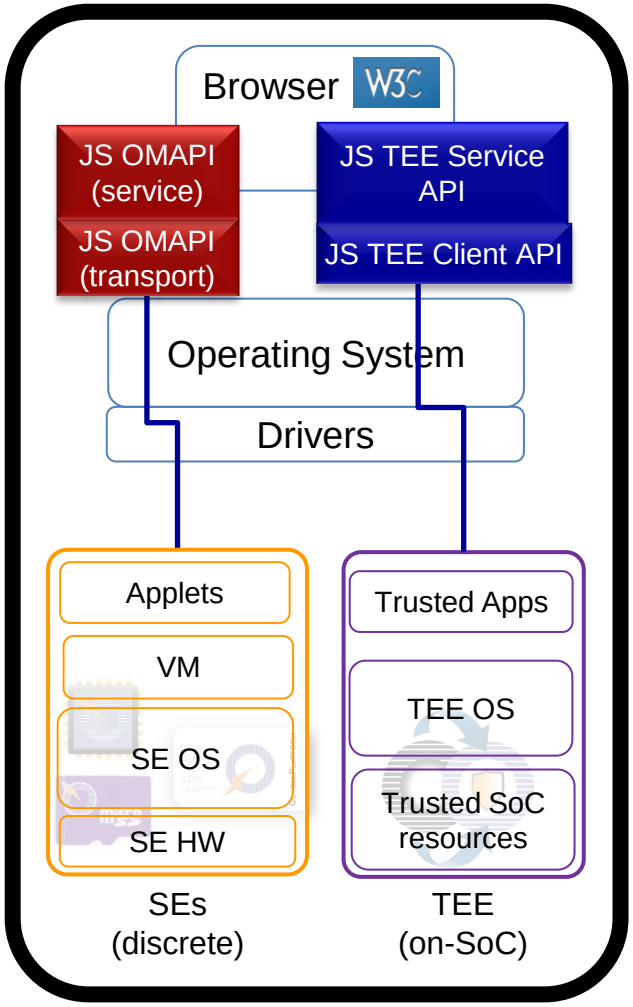
Interfaces to GP technologies

- TEE
  - TEE Client API: session management with a Trusted Application
    - Published in C,
    - JS binding available as draft (on hold)
  - TEE Functional APIs not specified yet
    - Access to services provided by the TEE
- SE
  - Open Mobile API: session management and functional services (SE discovery, secure storage, file system…)
    - Specification is language-agnostic
  - SE API in TEE: session management only (based on OMAPI), Secure Channel addition under drafting
- Access control enforcement
  - To TEE : OS security
  - To SE: SE Access Control



Proposals

- JS Open Mobile API (transport + SE discovery) and JS TEE Client API to manage sessions to SE/TEE
  - JS OMAPI may go through TEE or not (transparent to the client)
  - TEE JS Client API available as working draft of the TEE Spec WG
- JS Open Mobile API (service) and JS TEE Service API to provide access to SE/TEE services (crypto, secure storage…)
- Additional possible work items
  - Identification of security levels of SE/TEE
  - Additional TEE Service APIs for security UCs: Trusted UI, Trusted Video path (DRM)



Way of working

- For the browser APIS to GlobalPlatform Secure component, the Collaboration between both world is a key requirement for success :
  - Open-source group in GlobalPlatform with contribution of W3C members

  Or
  - W3C group with contribution of GlobalPlatform members

- Liaison between GP and W3C for the proposed work items to synchronize roadmaps.

Thank you!

herve.sibert@st.com

Access to the Experts! (Seminars)

GLOBALPLATFORM™

2nd Annual Trusted Execution Environment (TEE) Seminar
Tuesday, 30 September in Santa Clara, California

Pre-Seminar Technical Workshop on Monday, 29 September

GLOBALPLATFORM™
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

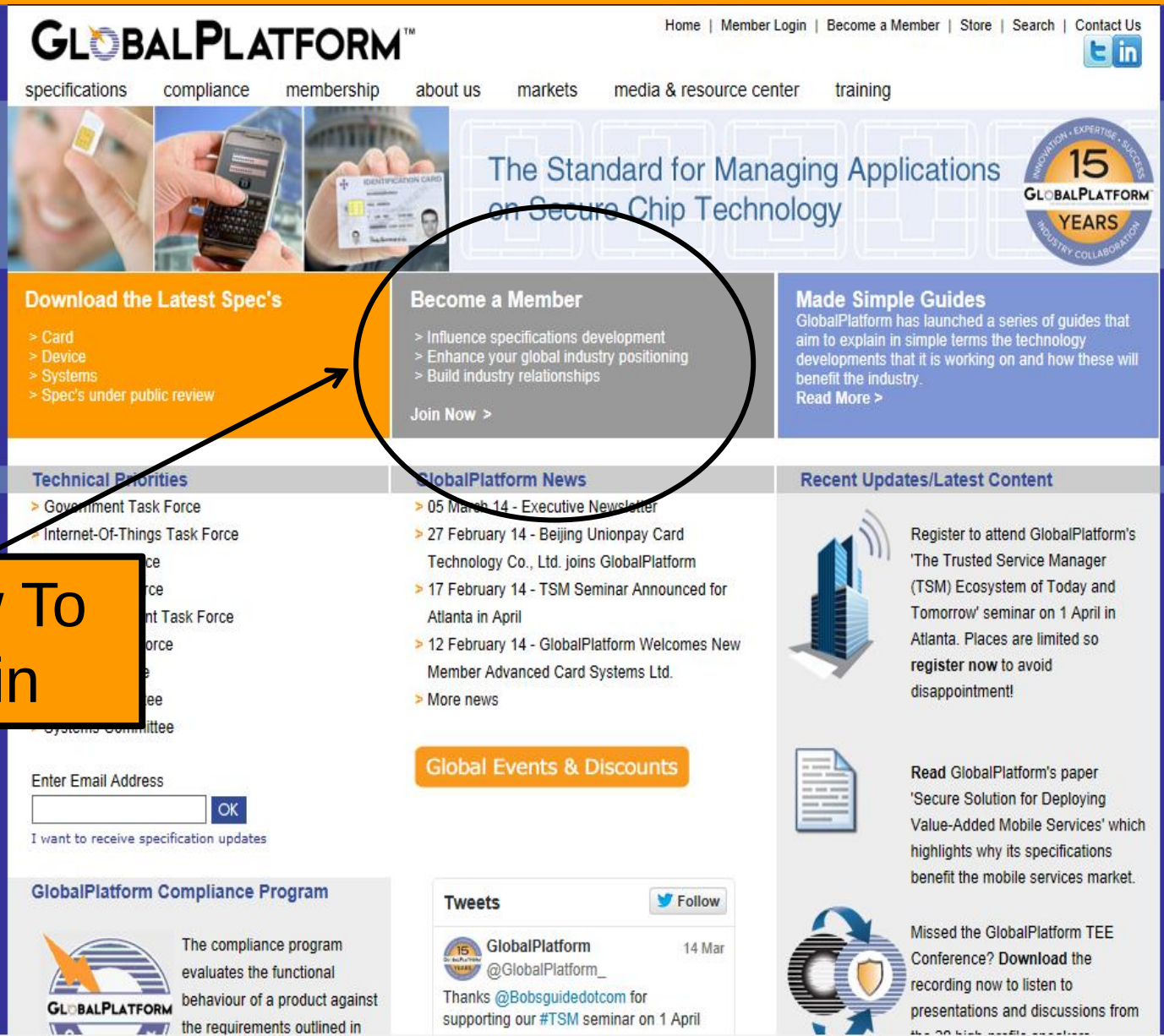
GlobalPlatform Presents:

THE TRUSTED EXECUTION ENVIRONMENT (TEE):

NEXT GENERATION MOBILE SECURITY FOR TODAY AND TOMORROW

Visit us @ www.globalplatform.org

GLOBALPLATFORM™



How To Join