

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 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

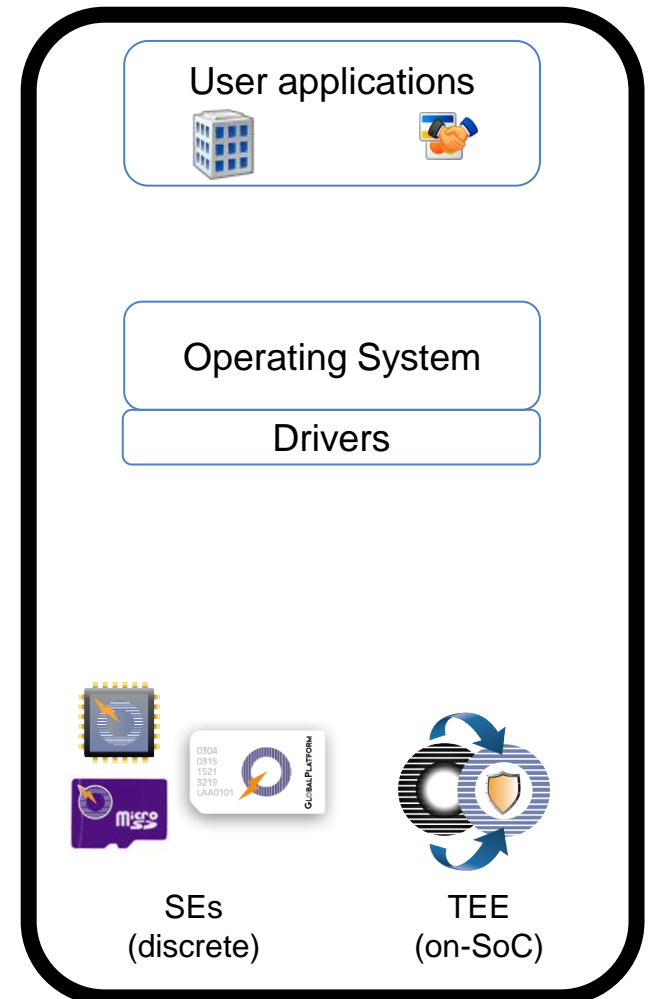


TRANSIT

- 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



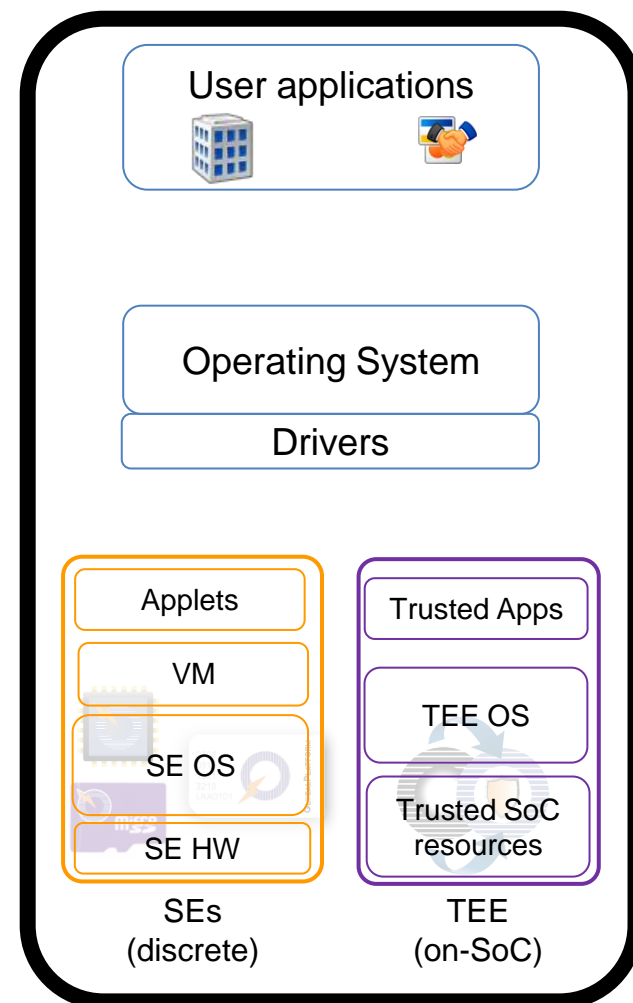
SE/TEE
head-end



- 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

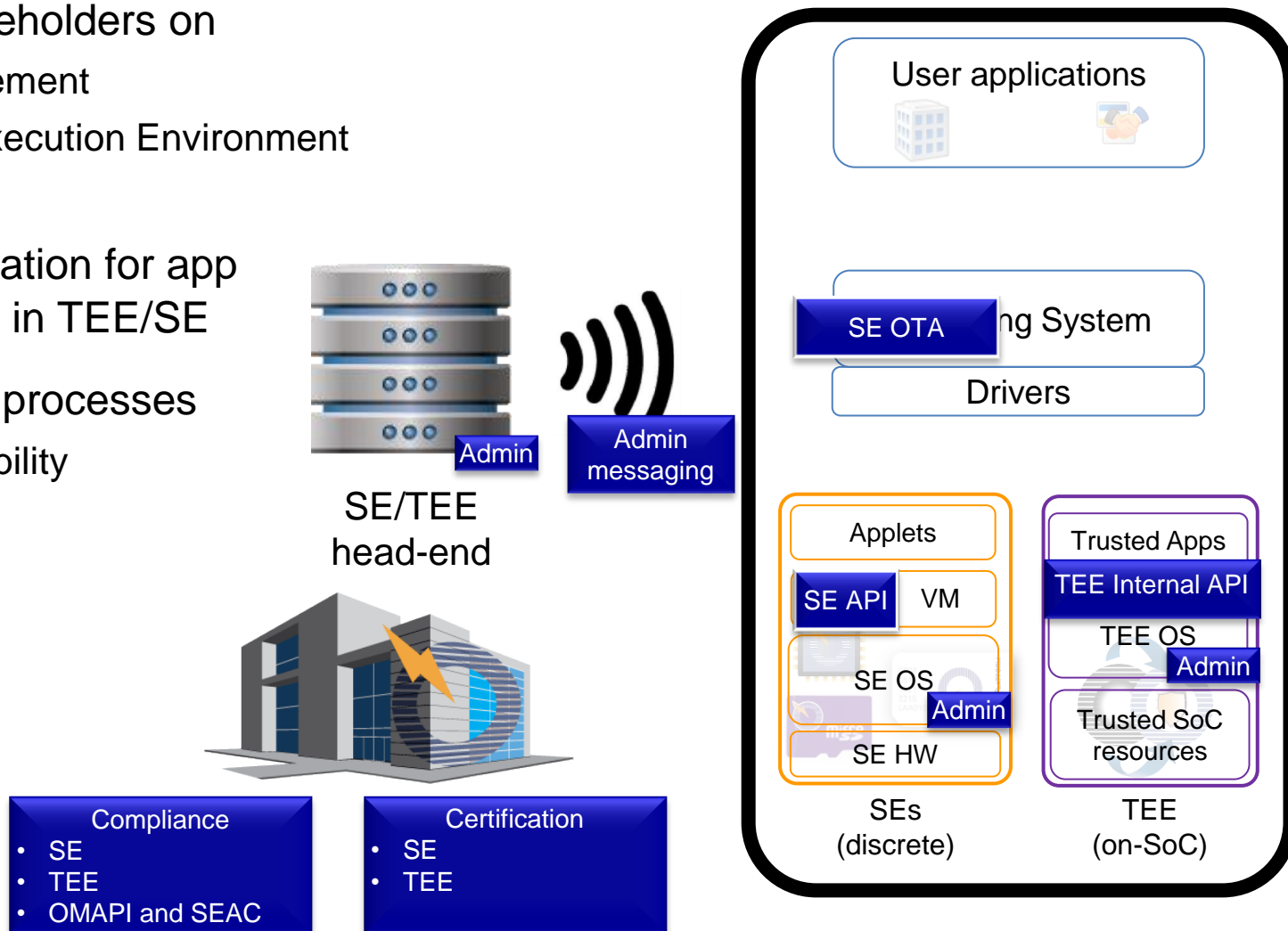


SE/TEE head-end

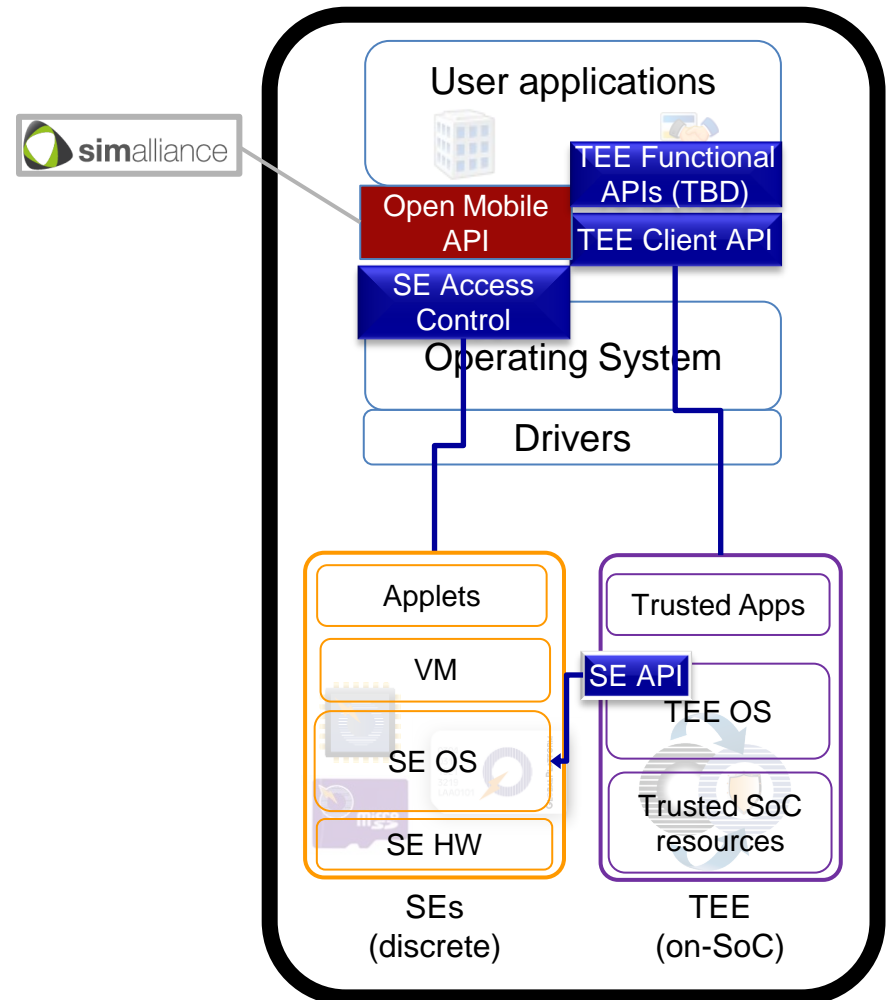


- Management of applications from multiple stakeholders on
 - Secure Element
 - Trusted Execution Environment (TEE)
- APIs specification for app development in TEE/SE
- Qualification processes
 - Interoperability
 - Security

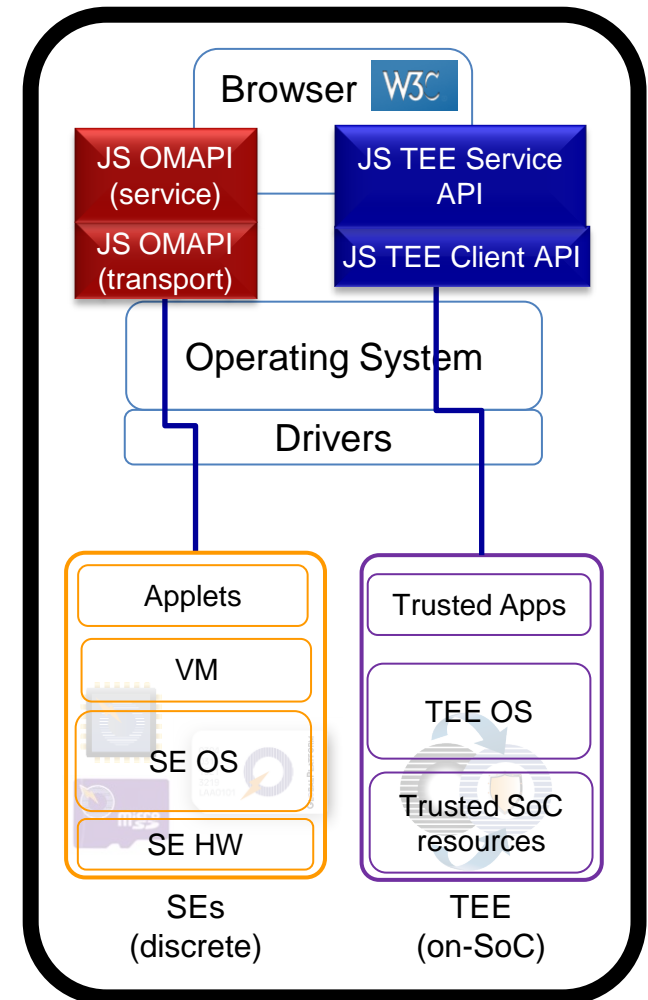
GlobalPlatform specifications



- 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



- 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)



- 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 membersOr
 - 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

Home | Member Login | Become a Member | Store | Search | Contact Us

specifications compliance membership about us markets media & resource center training



The Standard for Managing Applications on Secure Chip Technology



Download the Latest Spec's

- > Card
- > Device
- > Systems
- > Spec's under public review

Become a Member

- > Influence specifications development
- > Enhance your global industry positioning
- > Build industry relationships

Join Now >

Made Simple Guides

GlobalPlatform has launched a series of guides that aim to explain in simple terms the technology developments that it is working on and how these will benefit the industry.

Read More >


Technical Priorities


- > Government Task Force
- > Internet-Of-Things Task Force
- > ...
- > ...
- > ...
- > ...
- > ...
- > ...
- > ...
- > ...
- > ...


GlobalPlatform News

- > 05 March 14 - Executive Newsletter
- > 27 February 14 - Beijing Unionpay Card Technology Co., Ltd. joins GlobalPlatform
- > 17 February 14 - TSM Seminar Announced for Atlanta in April
- > 12 February 14 - GlobalPlatform Welcomes New Member Advanced Card Systems Ltd.
- > More news

Recent Updates/Latest Content

 Register to attend GlobalPlatform's 'The Trusted Service Manager (TSM) Ecosystem of Today and Tomorrow' seminar on 1 April in Atlanta. Places are limited so **register now** to avoid disappointment!

 Read GlobalPlatform's paper 'Secure Solution for Deploying Value-Added Mobile Services' which highlights why its specifications benefit the mobile services market.

 Missed the GlobalPlatform TEE Conference? **Download** the recording now to listen to presentations and discussions from the 20 high profile speakers


Global Events & Discounts

Enter Email Address


I want to receive specification updates


GlobalPlatform Compliance Program

The compliance program evaluates the functional behaviour of a product against the requirements outlined in



Tweets

 Follow

 GlobalPlatform @GlobalPlatform_ 14 Mar

Thanks @Bobsguidedotcom for supporting our #TSM seminar on 1 April

How To Join