

## Marc Vauclair

---

**From:** Shrinath.Eswarahally@infineon.com  
**Sent:** Tuesday, October 25, 2011 19:07  
**To:** Marc Vauclair; Rohit.Khera@sandc.com; mike.ahmadi@granitekey.com  
**Cc:** Shrinath.Eswarahally@infineon.com  
**Subject:** RE: UCA Embedded Systems Security - Device Security  
**Attachments:** Basic+Knowledge+EC2004.pdf; TPM\_Certification\_ProductBrief.pdf; Trusted+Computing+for+embedded+platforms.pdf; 20111025-SmartGridGatewayProtectionProfile-IntroEugenePolulyakh.pdf

Marc,

Due to my business travel, I will not be able to join this week's call on Thursday.. But Here is the following info on TPM stuff, as agreed..

1. The FAQ answers most questions about Embedded TPM sub group:  
[http://www.trustedcomputinggroup.org/?e=category.developerDetail&urlpath=embedded\\_systems&resource\\_type\\_id=-1&is\\_faq=true#nav\\_jump](http://www.trustedcomputinggroup.org/?e=category.developerDetail&urlpath=embedded_systems&resource_type_id=-1&is_faq=true#nav_jump)
2. Trusted Solutions:  
<http://www.trustedcomputinggroup.org/solutions>
3. TPM information:  
<http://www.infineon.com/cms/en/product/chip-card-and-security-ics/embedded-security/trusted-computing/trusted-platform-module-tpm1.2-pc/channel.html?channel=ff80808112ab681d0112ab6921ae011f>

In NIST CSWG TCC Workgroup, attached Smartgrid Gateway protection profile slides were presented..This Is just FYI, as we were also discussing this in Device security group..

Best Regards  
Shrinath.E.V.

---

**From:** OpenSG SG Security WG Embedded Systems Security Task Force [<mailto:OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG>] **On Behalf Of** Marc Vauclair  
**Sent:** Thursday, October 13, 2011 5:53 AM  
**To:** [OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG](mailto:OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG)  
**Subject:** UCA Embedded Systems Security - Device Security

Dear all,

For those of you that are not fortunate in reaching the Sharepoint, please find attached the minutes of the previous meeting.

They are also located here: <http://osgug.ucauiug.org/utilisec/embedded/Shared> Documents/Device Security/Meeting Minutes.

Regards,  
Marc

Marc Vauclair

BU Identification, Engineering/Architecture/Authentication, Smart IDs Networks  
Senior system architect and Technology Manager Security Applications, Senior Principal  
NXP Semiconductors  
Interleuvenlaan 80  
3001 Leuven, Belgium

Tel. +32 16 390 602 Mobile + 32 475 36 16 82 Fax +32 16 390 855

Email [Marc.Vauclair@nxp.com](mailto:Marc.Vauclair@nxp.com), [www.nxp.com](http://www.nxp.com)

PGP Fingerprint: FACC 4E8F E4A9 7AAA A9E8 F9CF 07B9 79A4 A66B EE0A

*I'll sleep when I'm dead*

The information contained in this message is confidential and may be legally privileged. The message is intended solely for the addressee(s). If you are not the intended recipient, you are hereby notified that any use, dissemination, or reproduction is strictly prohibited and may be unlawful. If you are not the intended recipient, please contact the sender by return e-mail and destroy all copies of the original message.

Unless otherwise recorded in a written agreement, all sales transactions by NXP Semiconductors are subject to our general terms and conditions of commercial sale. These are published at [www.nxp.com/profile/terms/index.html](http://www.nxp.com/profile/terms/index.html)