Intrinsic-ID enables secure boot software authentication

EINDHOVEN, THE NETHERLANDS – April 25, 2012 - The Dialog Semiconductor SC14453S is the world’s first commercially available Voice over IP (VoIP) processor circuit that integrates Intrinsic-ID’s patented Hardware Intrinsic Security IP – also referred to as Physical Unclonable Function (PUF).

In Hardware Intrinsic Security (HIS) technology a secret key is extracted like a silicon biometric or fingerprint from silicon hardware directly and only when required.
By using this HIS-based fingerprint a firm binding of software and hardware is possible, offering superior levels of anti-tampering and anti-cloning characteristics.

This approach can ensure that only authenticated software can run on the SC14453S platform. A message authentication tag for a bootloader or software image of a particular customer is securely stored with the HIS IP of Intrinsic-ID, without the need for embedded non-volatile memory.

“We selected Intrinsic-ID’s HIS technology because of its proven reliability, ease of integration and cost-effective silicon area footprint”, said RenéKohlmann, senior director at Dialog Semiconductor. “The resulting SafeKey solution for secure boot is programmable while at the same time providing authentication and top-level security”.
“Dialog Semiconductor takes a lead position in providing the highest level of security in the VOIP processor market”, said Tony Picard, VP Business Development at Intrinsic-ID. “OurHIS-based security IP enables Dialog Semiconductor’s customers to ensure the integrity of their differentiating software with the highest

level of anti-virus protection, through protecting their software with the electronic fingerprint that is unique for every device, making chips unclonable."

www.intrinsic-id.com [1]

Source URL (retrieved on *02/01/2015 - 12:42pm*): http://www.ecnmag.com/product-releases/2012/04/intrinsic-id-enables-secure-boot-software-authentication?qt-recent_content=0

Links:
[1] http://www.intrinsic-id.com