

INTRINSIC ID

Secure your digital life™



## ***Bringing trust to the mobile Cloud***

***Saturnus® Security Framework***

INTRINSIC ID

Confidential

Secure your digital life™

## Intrinsic ID

- Spin-out of Philips security team
- Leader in security IP and applications
  - Leader in Physically Unclonable Function technology (PUF)
  - Using *Hardware Intrinsic Security™*
- Headquarters in Eindhoven
- Operations in USA and Asia
- Privately held company
  - Prime Ventures
  - Robert Bosch Venture Capital

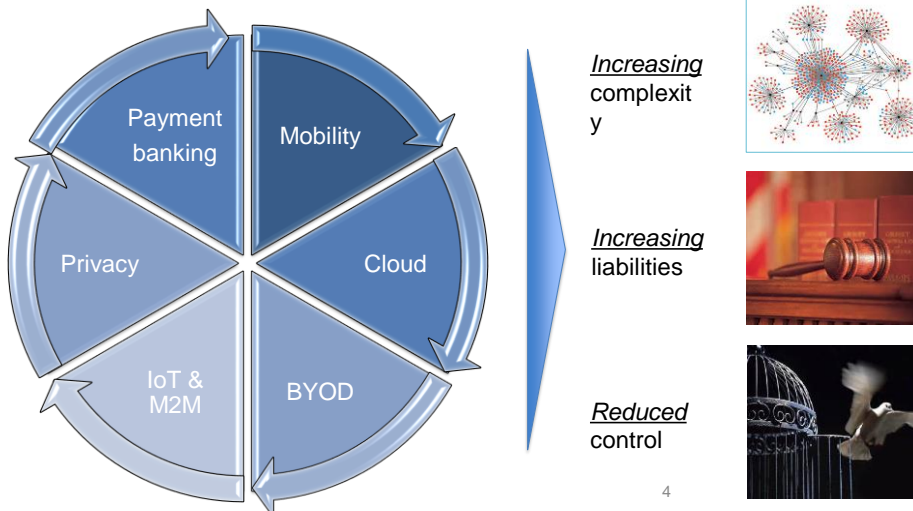


## Summary of proposal

- The Saturnus® Security Framework (SSF) is a framework for developing secure and convenient mobile and desktop applications.
- It provides hardware-level security to applications without the cost and logistical complexity of dedicated hardware solutions and while remaining independent from device manufacturers or mobile operators.
- It builds on Physically Unclonable Functions (PUF) an advanced security technology where Intrinsic-ID is the world leader
- Our SSF API gives developers access to a PUF secure element and has advanced functions to easily build applications that are easy to use and secure
- Use cases are: strong authentication, secure cloud access, mobile payment and banking

3

## Market trends seem to make security harder



4

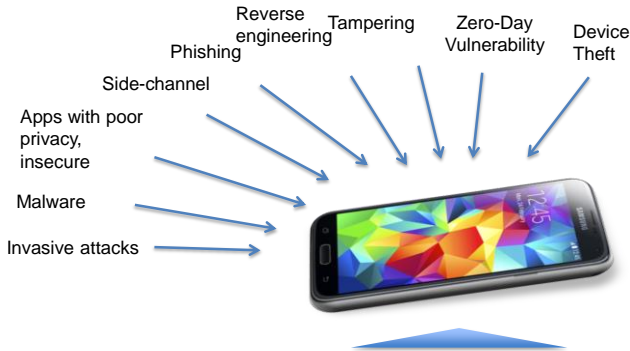
# INTRINSIC ID

Confidential

I want:

- Quick, easy access
- Own apps
- No passwords
- All on one device

## Strong need for endpoint security



- |                         |                        |
|-------------------------|------------------------|
| Credit card information | Corporate applications |
| Mobile banking access   | Cloud access           |
| Corporate VPN access    | Sensitive information  |
| Accounts and passwords  | Private information    |

# INTRINSIC ID

Confidential

Secure your digital life™

## Today: trade-off security, cost and convenience

€ Low cost    😊 convenient    🛡️ secure

**Authentication**

€ 😊

€ 🛡️

🛡️

**Online banking**

€ 😊

€ 🛡️

🛡️

**INTRINSIC ID**

Confidential

Secure your digital life™

IID brings addresses this challenge with secure and scalable solution based on existing hardware

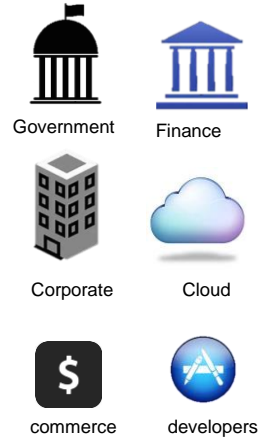
**PUF enabled phone**



PUF: Physically Unclonable Function



**Market Opportunities**



**INTRINSIC ID**

Confidential

Secure your digital life™

SRAM PUFs provide an excellent root of trust

**Due to deep sub-micron process variations ICs are intrinsically unique**

**Start-up SRAM values establish a unique and robust fingerprint**

**The fingerprint is turned into a secure secret key which is the foundation of enhanced security**

- PUF properties**
- Strong entropy, high randomness keys
  - Unclonable, tamper-proof
  - No keys at rest
  - Enables independent Root-of-Trust

- IID Technology Benefits**
- Based on SRAM available in every device
  - No custom design needed
  - Tested and vetted for defense markets
  - Proven, robust and scalable technology
  - Available in mobile phones, USB dongle
  - Protected by over 20 patents

**INTRINSIC ID**

Confidential

Secure your digital life™

**IID is already successfully used in embedded systems**

Segments covered	Design wins	Products deployed
 Mobile  G&D  smartcard  automotive  telecom  content	 <b>Microsemi</b>  <b>NXP</b>  <b>Panasonic</b>  <b>THALES</b>  <b>irdeto</b>  <b>inside SECURE</b>  <b>SELEX</b>  <b>RENEASAS</b>  <b>Coherent Logix</b>  <b>ST</b> 	 <b>Quiddikey</b> Secure key management  <b>Confidentio-sc</b> Integrated security processing  <b>Quiddicard</b> Key programming

**INTRINSIC ID**

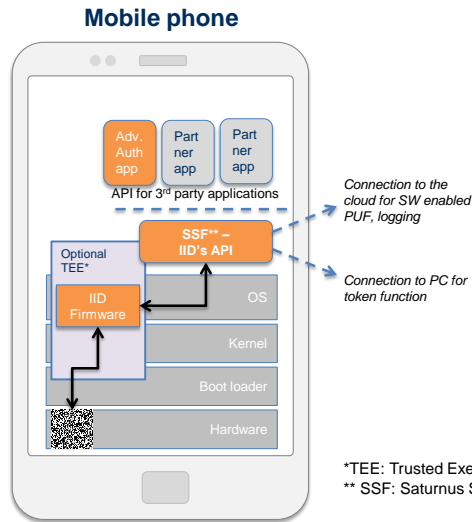
Confidential

Secure your digital life™

**Now: Strong Authentication with IID in flagship phones**

 <b>INTRINSIC ID</b> Confidentio™-sc Intrinsic-ID IP   Uninitialized SRAM data within the mobile	<p>Enabling high quality, securely stored PUF-based Keys</p> 	<p>Combining mobile OEM and Intrinsic ID's government vetted technology</p> <p>Strongest security on mobile device</p> <p><i>Natively implemented in flagship Android phones</i></p> <p><b>Available: Q4-2014</b></p>
---	--	---

## Developers can build secure apps with PUF via our API



### SSF API



- User friendly API for developers
- Strongest root of trust with IID's PUF technology
- Provides:
  - key generation, storage, retrieval
  - encryption, decryption
  - device authentication
  - digital signing
  - key programming

\*TEE: Trusted Execution Environment

\*\* SSF: Saturnus Security Framework – our API

## Enabling convenient, flexible and secure applications



**No Interaction:**  
Convenient Authentication based on device proximity

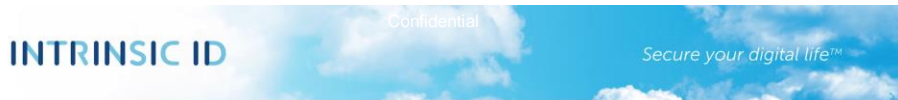


**Simple interaction:**  
Convenient Authentication based on device & button



**Natural Interaction:**  
Convenient 2F auth. With device and biometric





## Use Case: Saturnus® secure cloud application

- Application for mobile & PCs
- Data encrypted before leaving device
- Direct from mobile or via PC
- Benefits of PUF
  - Strong, locally generated keys
  - Keys are securely stored
  - Keys cannot be transferred to another device (even when rooted)
- End user benefits
  - Use public cloud services while keeping full privacy
  - Transparency & convenience



13



## Use case: Saturnus® strong authentication

- Strong two factor authentication
- For enterprise, cloud and PC
- Benefits of PUF
  - No secret stored
  - Based on device DNA (PUF)
  - Unclonable authenticator
- End user benefits
  - Convenience: phone as token
  - Secure: strong device authentication



14



# INTRINSIC ID

*Secure your digital life™*

## Questions

More information: [www.intrinsic-id.com](http://www.intrinsic-id.com)  
Pim Tuyls [pim.tuyls@intrinsic-id.com](mailto:pim.tuyls@intrinsic-id.com)  
Luis Ancajas [luis.ancajas@intrinsic-id.com](mailto:luis.ancajas@intrinsic-id.com)  
Boris Kennes [boris.kennes@intrinsic-id.com](mailto:boris.kennes@intrinsic-id.com)

15



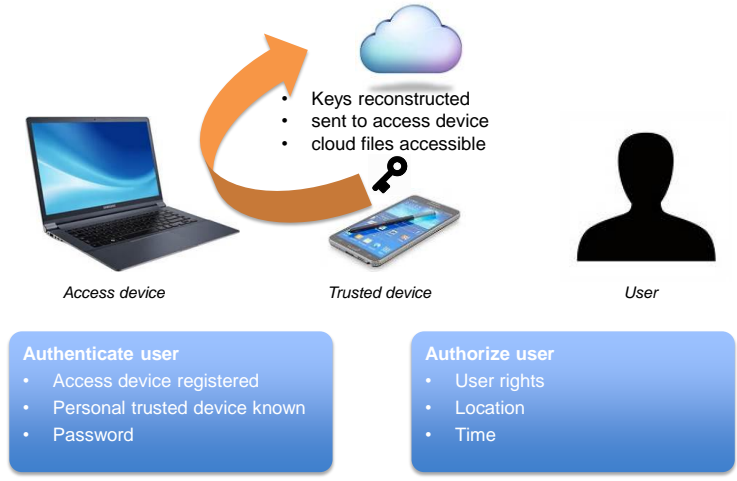
## BACK-UP

16

INTRINSIC ID Confidential

Scheme enables bank to use public cloud in banking operations

Combined use case: remote access to sensitive corporate data in public cloud



INTRINSIC ID Confidential Secure your digital life™

Saturnus® secure cloud application on mobile

Log into your account

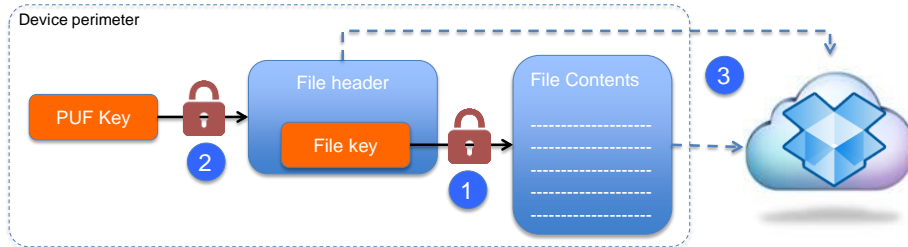
Browse your files

Read your files

Keep them hidden from others



## Simplified operation of Secure Cloud app



### Main operations

1. File is encrypted with random file key
2. File key is wrapped using the PUF key and included in the file header
3. File (including header) sent to Dropbox

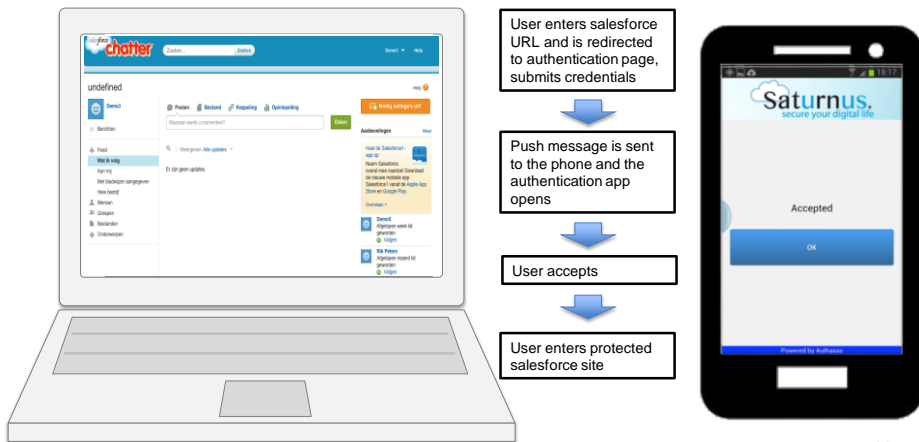
### Benefits:

- File headers can only be decrypted with a user-specific key that is securely stored with PUF
- The application accesses the PUF via the easy to use Saturnus® Security Framework API
- Data in the cloud can only be accessed by enrolled device
- Keys are securely stored and cannot be cloned (even when device is rooted)

19



## Saturnus® strong authentication with Salesforce



20

# INTRINSIC ID

Confidential

## Detailed flow

