UiO : University of Oslo

FIDO Trust Requirements

Ijlal Loutfi, Audun Jøsang
University of Oslo
Mathematics and Natural Sciences Faculty

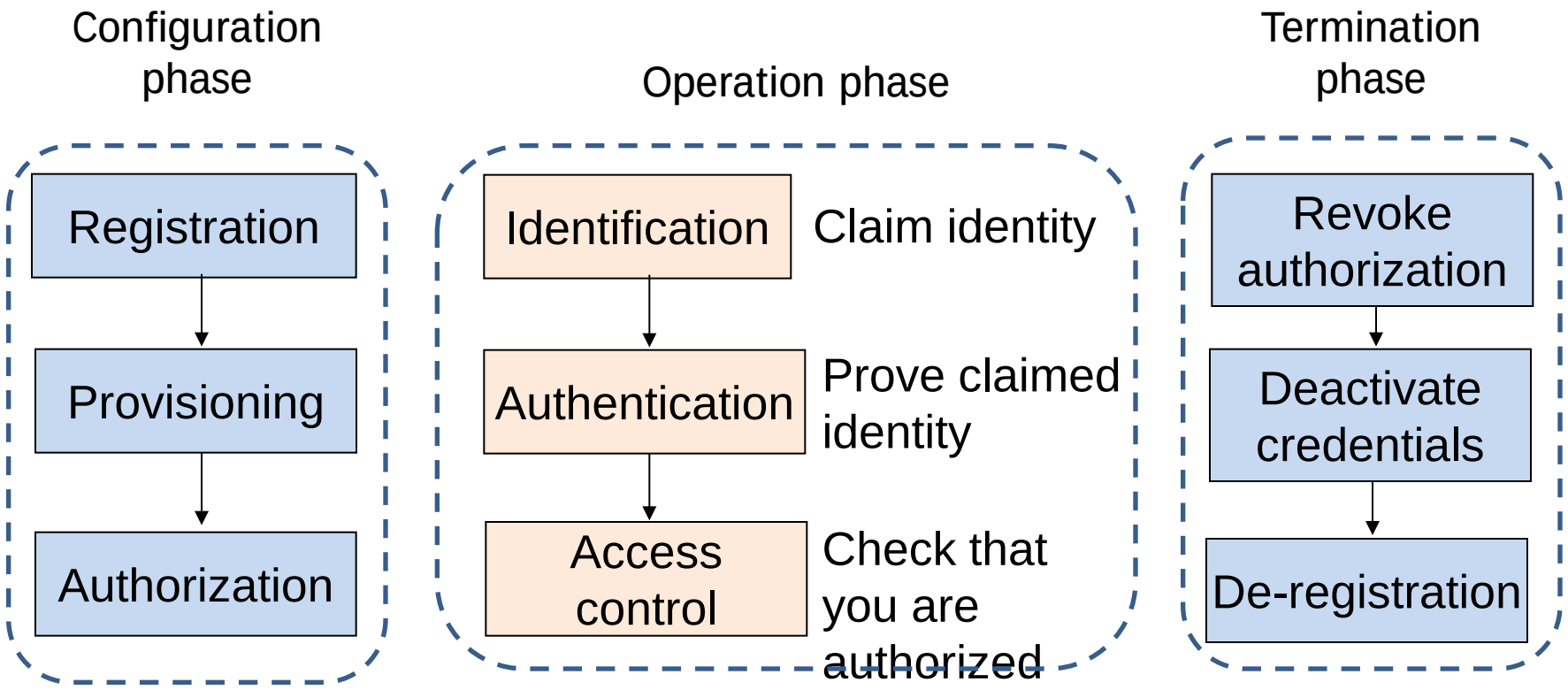
NordSec 2015,Stockholm, Sweden
October, 20th 2015

Working assumption:
End Users' Platforms **are** compromised
or
are going to be compromised

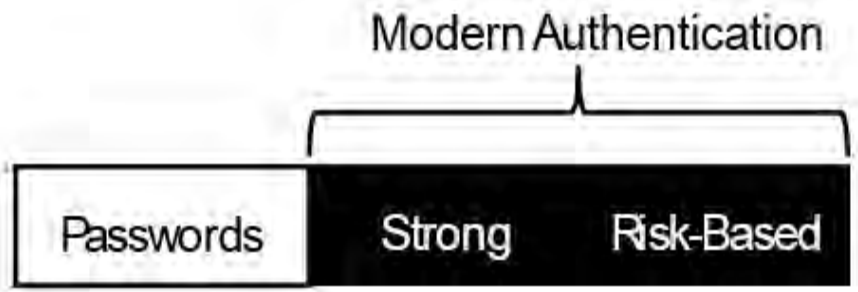

VISA
Microsoft
SAMSUNG
NETFLIX
RSA
Bank of America
egis Technology
MasterCard
IdentityX
DELL
LG Electronics
PayPal
Google
infineon
salesforce
DISCOVER
Nok Nok LABS
lenovo FOR THOSE WHO DO.
oberthur TECHNOLOGIES THE M COMPANY
ARM
BlackBerry
aetna
eyeLock
Ping Identity
AGNITIO
IDEX THE ID OF YOU
Medimpact Healthcare Systems
Synaptics
fido alliance
SafeNet
THE DATA PROTECTION COMPANY
GO-Trust Trust in a Mobile World
ib INTEGRATED BIOMETRICS
SurePass id
AUTHENTIFY
SECURE KEY
toopher
NXP
ca technologies
Entersekt
wave
yubico Trust the Net.
insyndia imagine. ignite. inspire.
DIAMOND FORTRESS TECHNOLOGIES
CrucialTec
FINGERPRINTS
IT'S ME!
Goldman Sachs
ARXAN Protecting the App Economy
BIO-key
natural security
CROCUS Technology Blossoming future
FingerQ www.fingerq.com
Facebanx
certus
CLOUDSECURITY CORPORATION
Allweb Technologies

Windows10
Alipay
Samsung Galaxy
Bank of America(for iOS and android users)
UK Government

Identity and Access Management (IAM) Phases

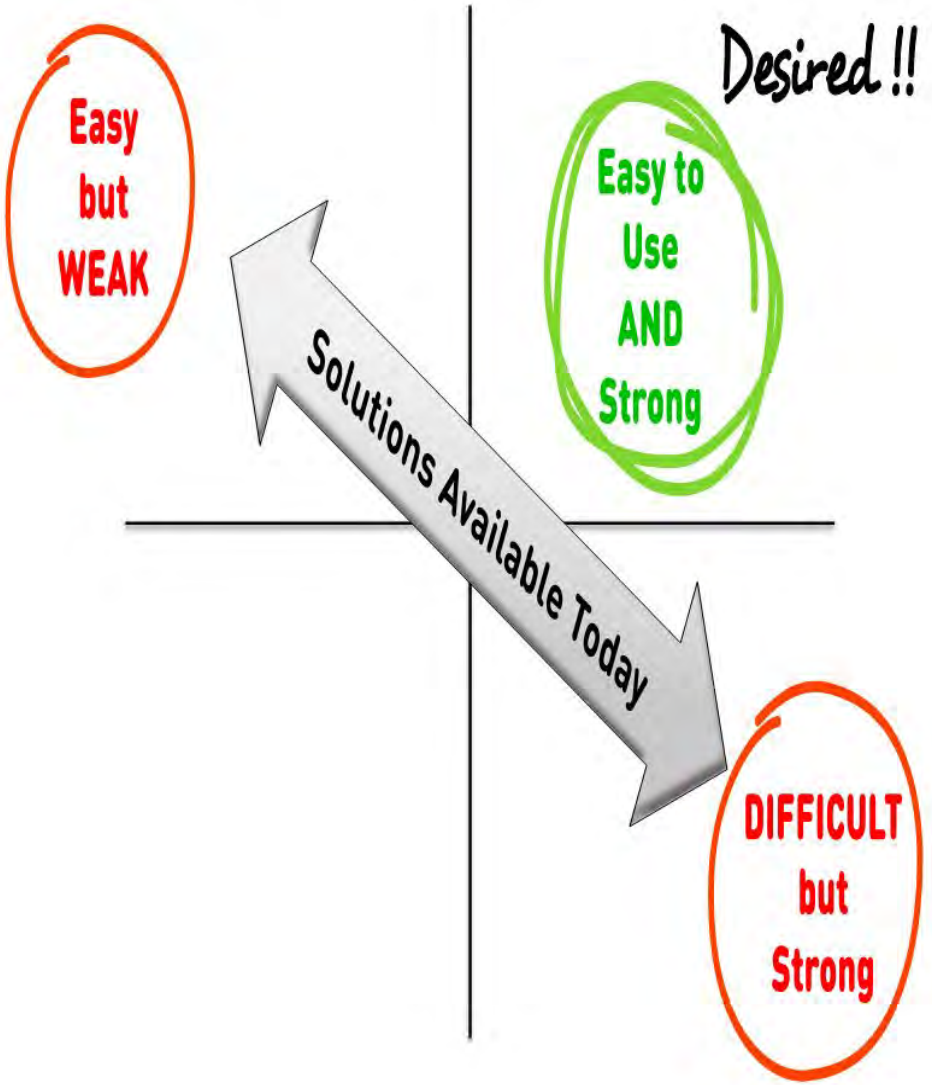


What this paper is not about



How and Why is Authentication challenging?

TODAY'S AUTHENTICATION SOLUTIONS FALL SHORT



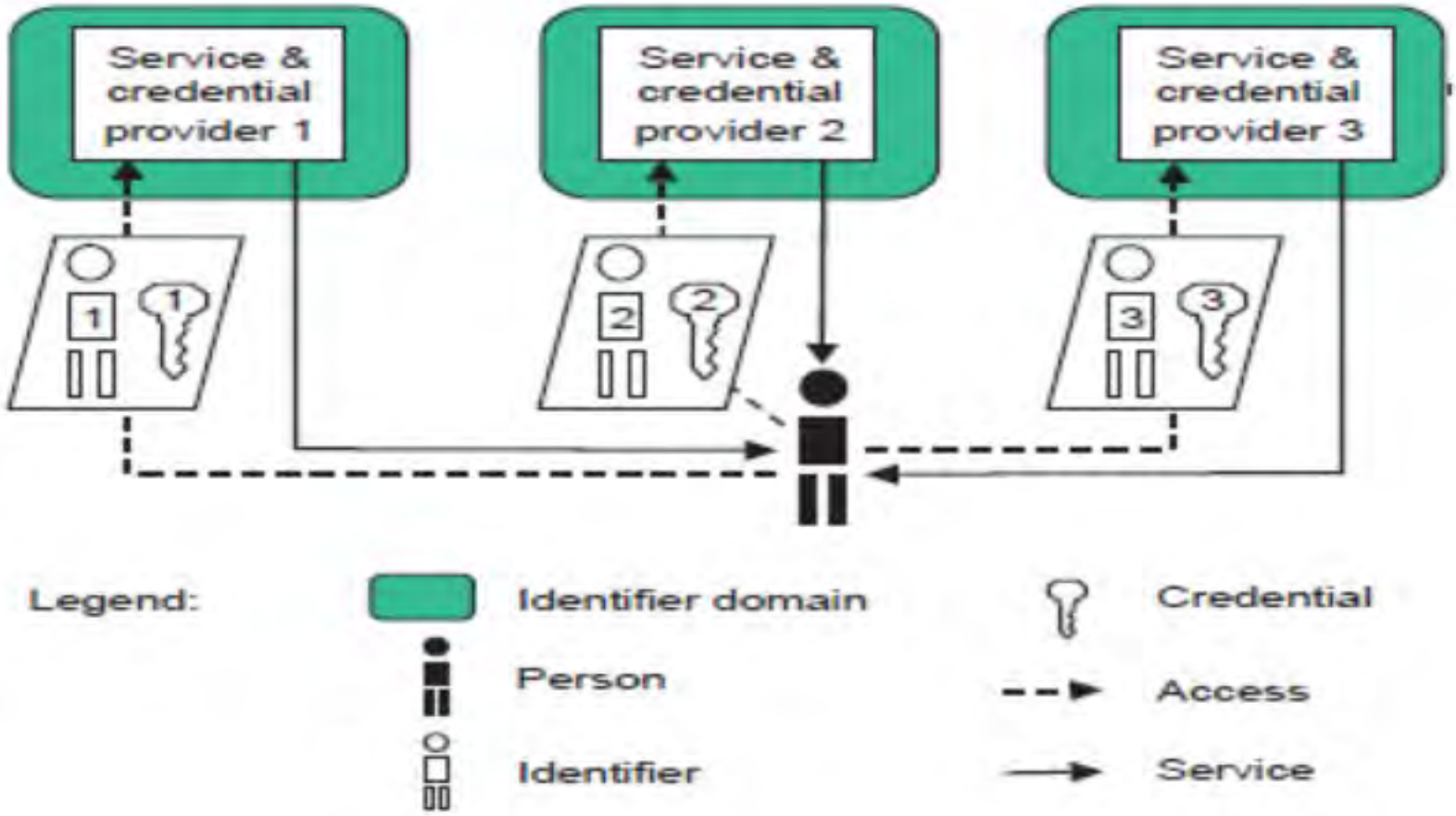
Trust?
Assurance?

Under what conditions?
What are its requirements?
By whom?
To whom?

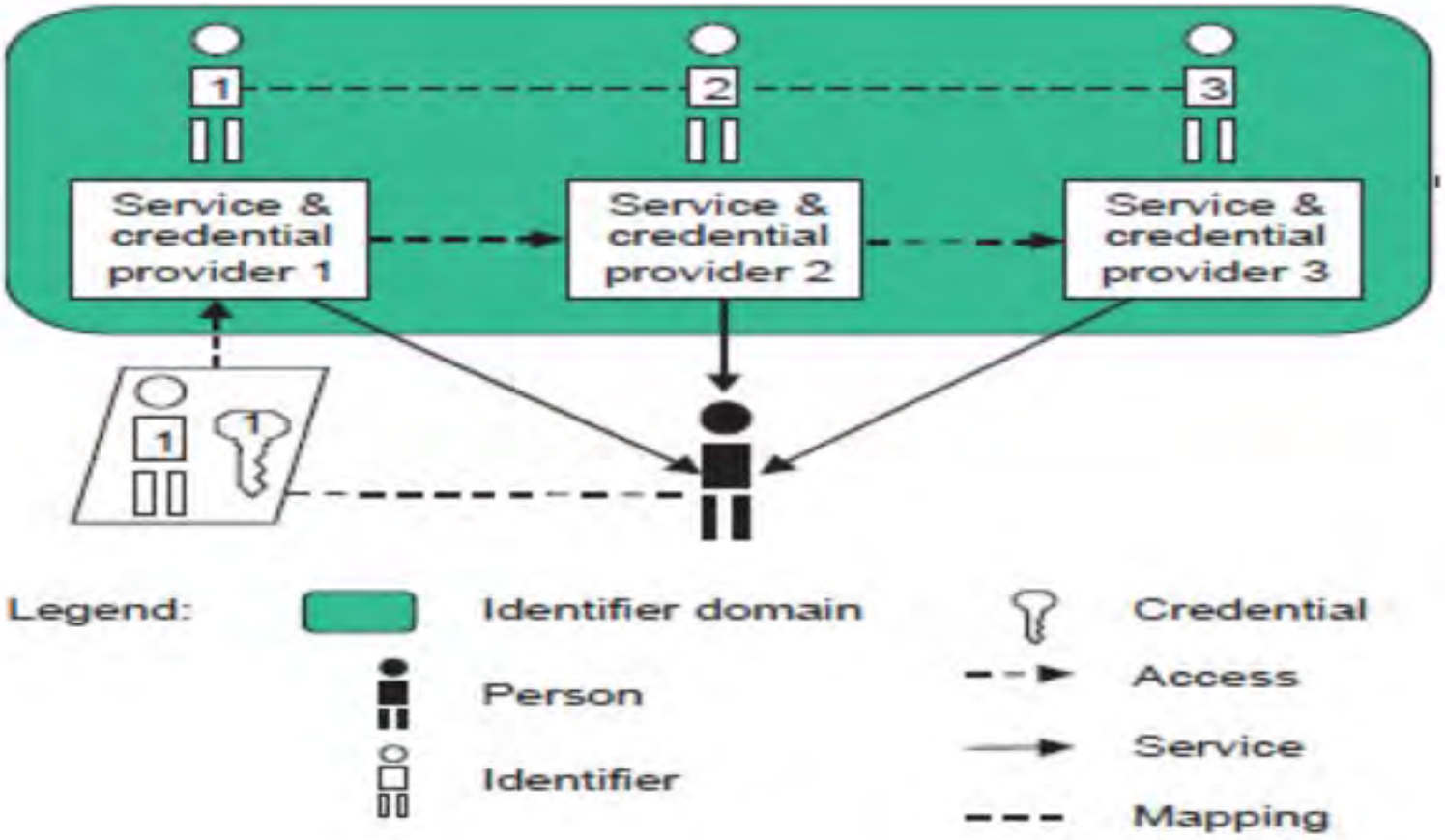
Current Authentication

1. Online **isolated** identity management.
2. Online **Federated** isolated identity management.
3. Offline Local device identity management.
4. Fast Identity Online (FIDO).

Online Isolated Authentication



Online Federated Authentication

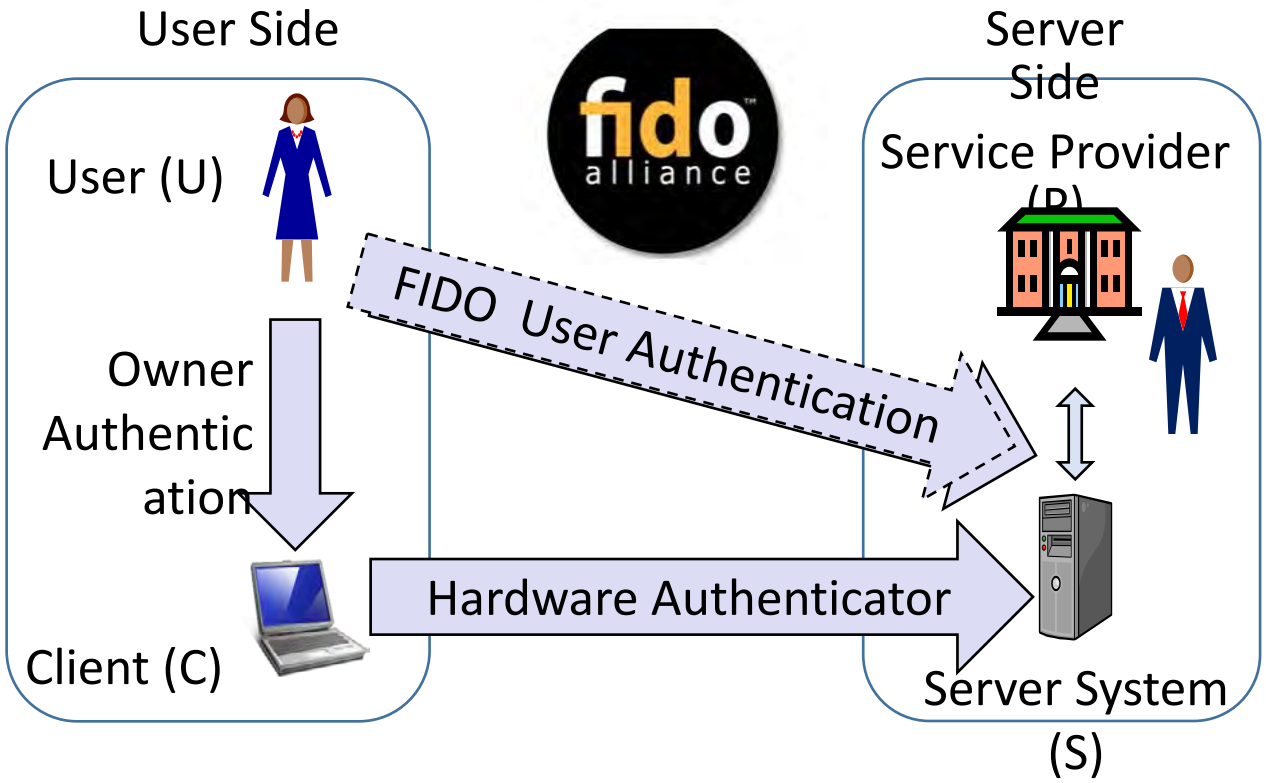


Offline Local Device Authentication

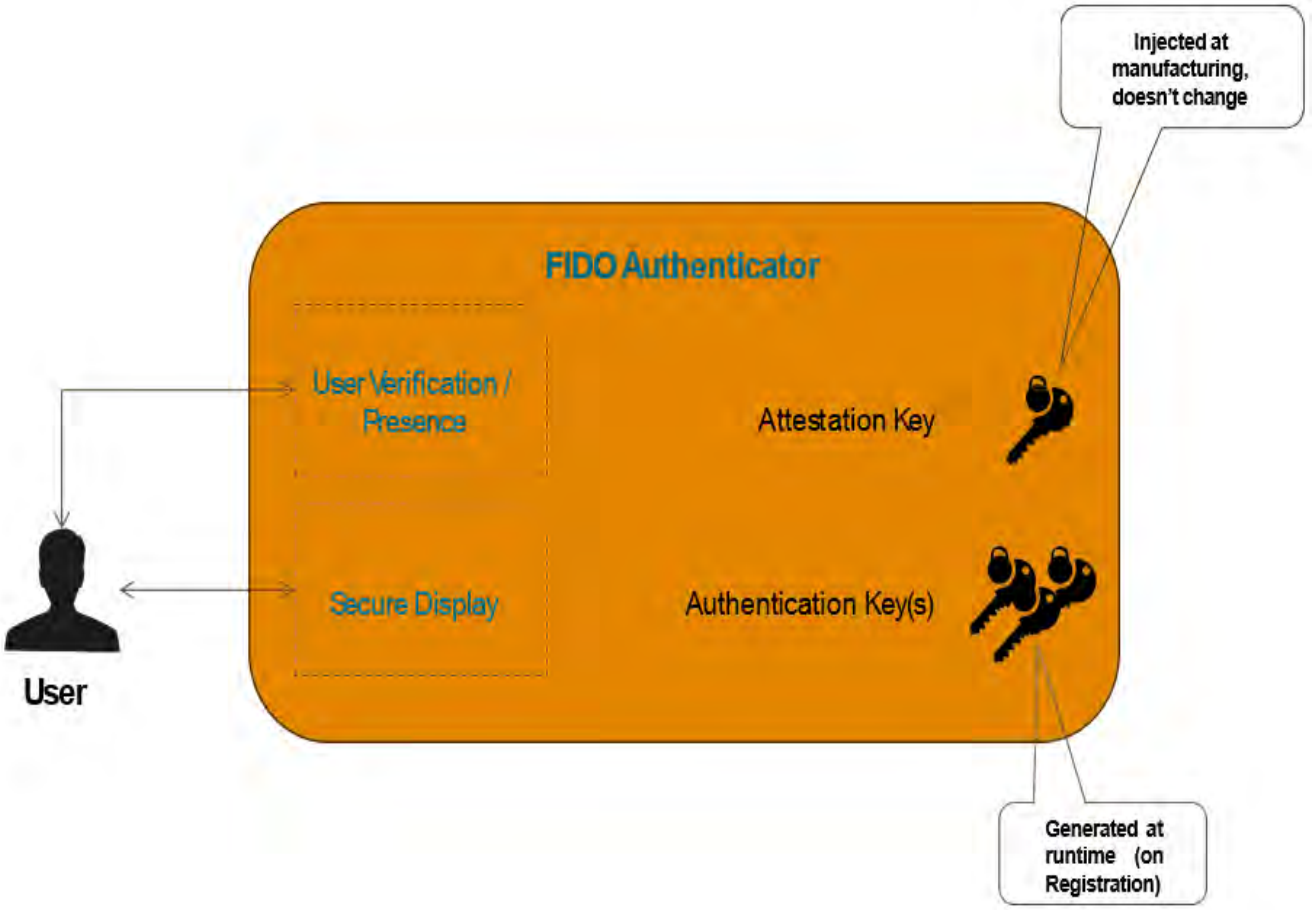
FIDO: Putting it Together

- The problem:
  - Simpler Stronger Online Authentication
- The Trend:
  - Simpler Stronger Offline Local Authentication
- Why Not:
  - Use Offline Local Authentication for Online Authentication.
  - This is the **core idea** behind FIDO standards.

FIDO: Authentication Scenario



Authenticator concept

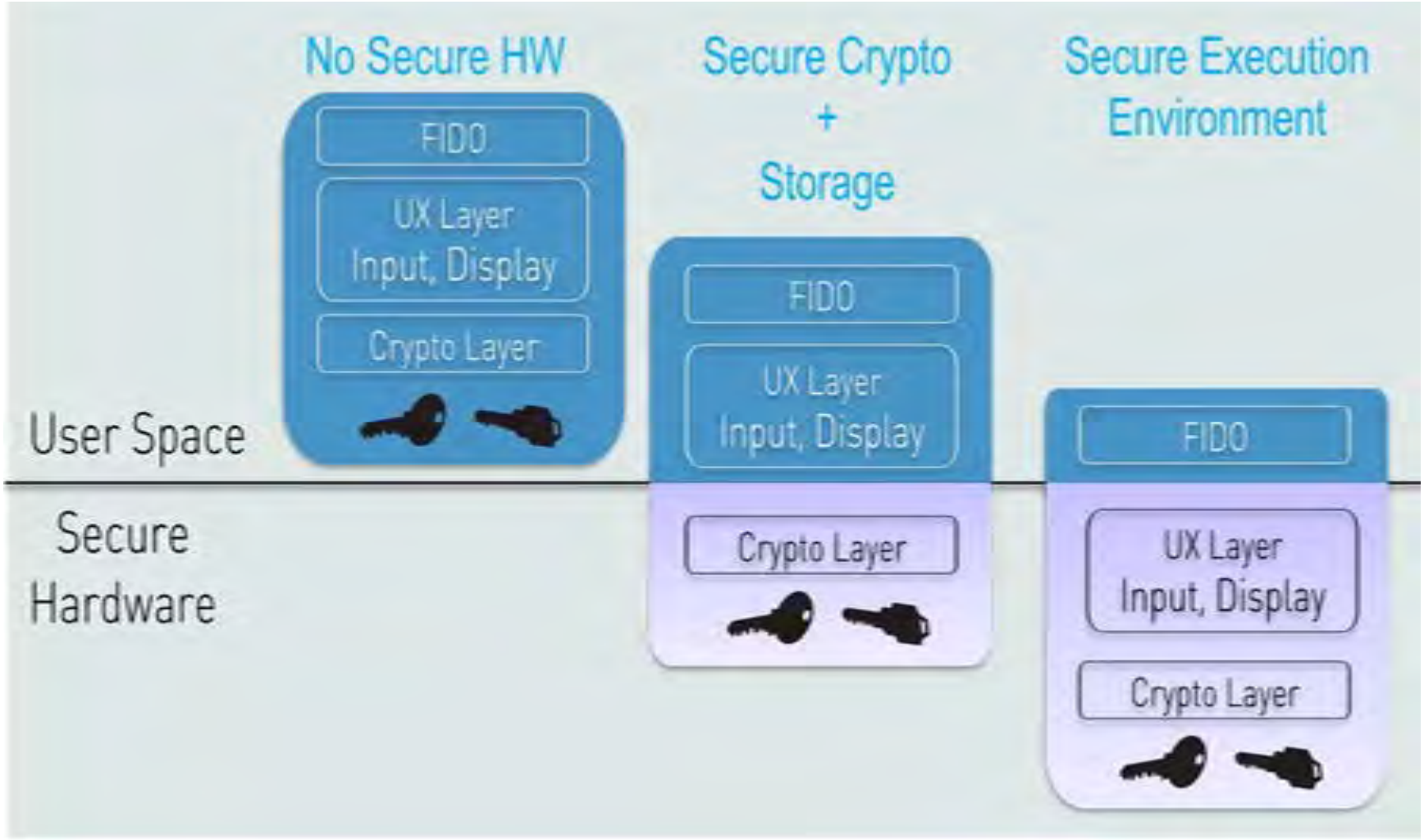


FIDO Authenticator Concept

It is expected that users will acquire FIDO Authenticators in various ways:

- Embedded in the platform
- Purchased
- Given by a service provider

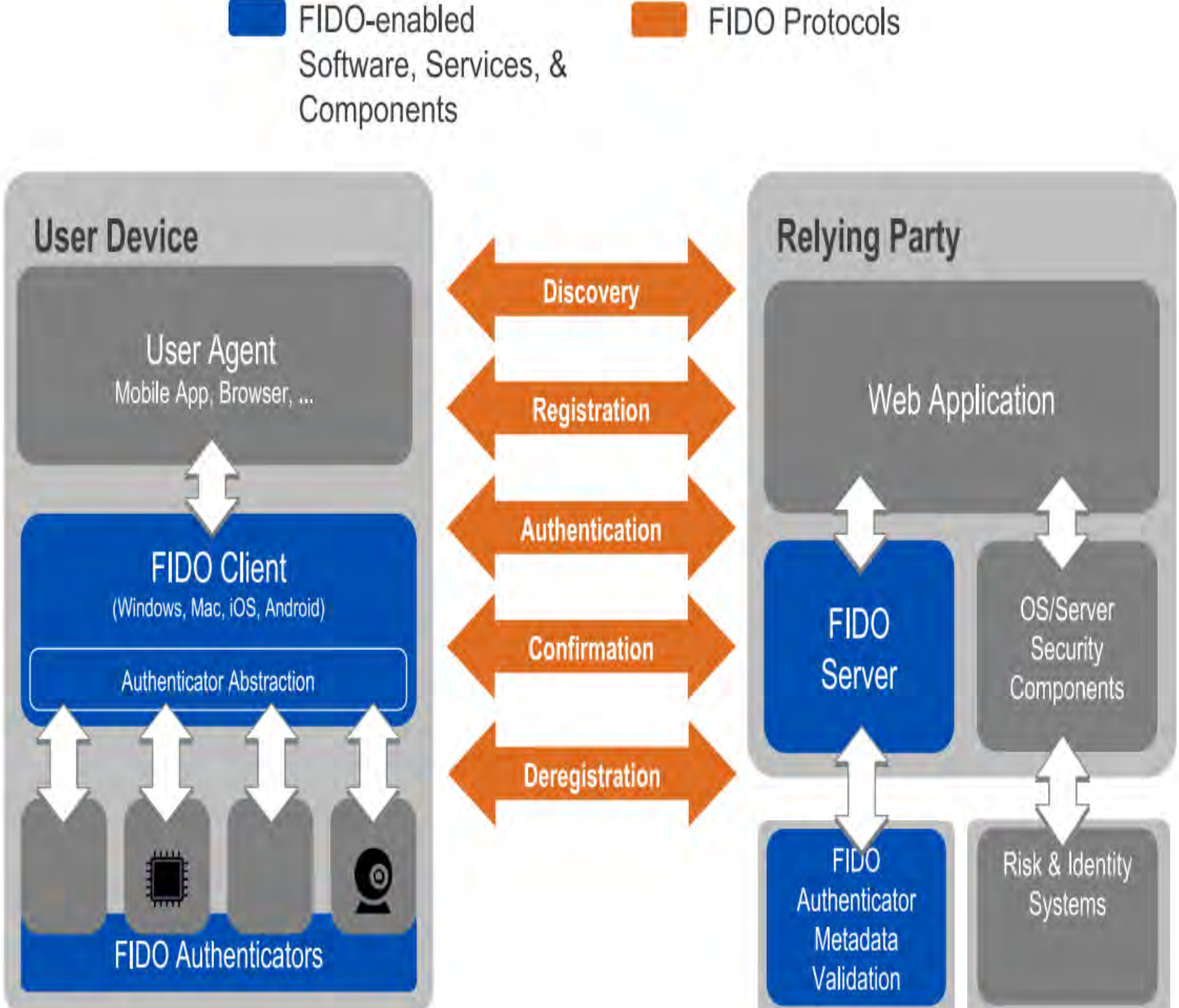
Choice of Security Profiles



FIDO Authenticator Concept

Examples:

- A fingerprint sensor built into a mobile device.
- A PIN authenticator implemented inside a secure element.
- A USB token with built-in user presence verification.
- A voice or face verification technology built into a device.


FIDO-enabled Software, Services, & Components
FIDO Protocols
User Device
User Agent
Mobile App, Browser, ...
FIDO Client
(Windows, Mac, iOS, Android)
Authenticator Abstraction
FIDO Authenticators
Discovery
Registration
Authentication
Confirmation
Deregistration
Relying Party
Web Application
FIDO Server
OS/Server Security Components
FIDO Authenticator Metadata Validation
Risk & Identity Systems

Online Identity Management Trust Requirements

The concept of Trust

Trust management

becomes a component of IdM

whenever different parties rely on each other for identity provision and authentication.

Isolated Authentication Trust Requirements

- The trust requirements between users and SPs are well understood
- The industry has had several decades of experience with this model, and users are familiar with it.
- Identifier provider, credentials provider and SP are the same:
  - The client and SP only need to trust each other for a small set of purposes

Isolated Authentication Trust Requirements

Client Trust in Service Providers:

1. The SP has the expected identity.
2. The SP protects client privacy.
3. The SP has implemented satisfactory user registration procedures and authentication mechanisms (from the clients perspective).

Service Provider Trust in Client:

1. The client handles their authentication credentials with adequate care.

Trust Requirements of Federated Online Identity Management

1. Trust between Federated Service:
   (a) Service access by assertions between SPs on behalf of users will only take place when legitimately requested by the client.

2. Trust in the Identity Mapping:
   (a) The mapping of identities between service providers is correct.

3. Client Trust in Service Providers:
   (a) The service provider adheres to the accepted policy for correlating personal data about the same client from other service providers.

FIDO Trust Requirements

Trust in :

1. FIDO consortium.
2. Trust in service providers.
3. Trust in hardware manufacturer.
4. Trust local device computing platform.
5. Trust in end users.
6. Trust in FIDO protocols.

Trust in Local Device Computing Platform

- The currently deployed online IdM solutions focus on defining more secure communication protocols between their end points (client, SP server, identity provider server).
- The question of whether the client computing platform (e.g.: computer, mobile phone) end users use to connect to SPs is compromised or not has been left out from their solutions.

Trust in Local Device Computing Platform

T10: *Trust that the user computing platform is not compromised by malicious software.*

Trust in Local Device Computing Platform

31.63 percent of the worlds PCs are infected with some sort of malware (Q2 2012) of 78.92 percent are Trojans.

- Even with the most carefully designed communication protocol between end points, and the most safely guarded server platform, the password of end users can still be compromised if they are authenticating to their SPs from a compromised device

- FIDO supports authenticators that are implemented as part of the computing platform.

Trust in End users

T11: *Trust the user will not expose his or her device to compromise in infected platforms.*

Trust in Service Providers

- SPs have the right to enforce policies about the type of authenticators they want their users to use while consuming their services:
  - SP authentication policy: a JSON data structure that allows a SP to communicate to a FIDO Client the capabilities or specific authenticators that are allowed or disallowed for use in a given operation.
  - The client then responds with an attestation certificate
  - It is then the responsibility of the SP to ensure how genuine this claim is, by using information in his metadata store.

Trust in Service Providers

T5: *Trust that the SP is able to correctly assess the risk level associated with the usage of his service by all his users.*

T6: *Trust that the SP establishes the appropriate network connection while updating the metadata store.*

Trust in Hardware Manufacturers

- Providing cryptographic evidence to the SP attesting to the type and provenance of the authenticator.

- The UAF specifications require implementers to ship UAF authenticators with the same attestation certificate and private key in batches of 100,000 or more in order to provide unlinkability [2].

Trust in Hardware Manufacturers

- T7: *Trust that hardware providers will not unintentionally break the unlinkibality property*.

- T8:*Trust that hardware providers will not intentionally break the unlinkibality property.*

- T9: *Trust that hardware manufacturers will not keep a backdoor in the authenticator,*

Trust in FIDO Consortium

- The FIDO consortium is responsible for certifying FIDO authenticators, and managing the certificate PKI.
- Certification refers to the FIDO program that allows members and non-members to measure compliance and ensure interoperability among products and services that support FIDO specifications.
- In the case of a FIDO authenticator that iscertified, it will be characterized by a set of metadata information. This metadata is associated with an AAID (Authenticator Attestation ID) and available from the FIDO Alliance

Trust in FIDO Consortium

- T1: *Trust that the FIDO consortium has identified the right set of metadata characteristics that are sufficient to identifying authenticators in ways that are meaningful to SPs to accept or reject them.*

- T2:*Trust that the certification is still meaningful throughout the time it is valid.*

- T3:*Trust that the FIDO consortium is able to detect and report authenticators breaching the metadata characteristics declared in their certification process, and update the metadata store accordingly.*

.

Trust Requirements	FIDO	Iso-lated	Fed-er-ated
The SP protects client privacy.		✓	✓
The SP has implemented satisfactory user registration procedures and authentication mechanisms.	✓	✓	✓
The client handles their authentication credentials with adequate care.	✓	✓	✓
Trust in the SP: ability to correctly assess the risk level associated with the usage of his service by all his users.	✓	✓	✓
Trust in the computing platform:it's not compromised by malicious software.	✓	✓	✓
Trust the user will not expose his device to compromise in infected platforms.	✓	✓	✓
Service access on behalf of users will only take place when legitimately requested by the client.	✓		✓
The SP adheres to the accepted policy for correlating personal data about the same client from other SPs.	✓		✓
Trust in FIDO consortium: it has identified the right set of meta-data.	✓		✓
The SP has the expected identity.	✓	✓	✓
Trust between Federated Service.			✓
Trust in the Identity Mapping.			✓
Trust in FIDO consortium: certificate is still meaningful throughout its lifetime.	✓		
Trust in FIDO consortium: its ability to detect and report authenticators breaching the metadata characteristics declared in their certification process, and update the meta-data store accordingly.	✓		
Trust in FIDO consortium: validity of the FIDO PKI used.	✓		
Trust in Hardware manufacturers: they will not unintentionally break the unlinkability property.	✓		
Trust in Hardware manufacturers: they not intentionally break the	✓		

Analysis

- *New Trust Requirements:*
  - FIDO has introduced trust issues that were not present in the previous online IdM solutions:
    - Authenticator hardware manufacturers The FIDO consortium.
- *Inherited Trust Requirements:*
  - *Trusting the computing platform.*
    - remember: the end user secret key is not stored on the server side, but rather on his own authenticator, which has to be connected to his possibly compromised computing platform.

Analysis

- FIDO Claim: make authentication both more usable and stronger.

instead of solving the trust requirements

of the previous online IdM solutions, FIDO has just shifted them to other components in its architecture

Analysis

- FIDO has created a more complex ecosystem, with new components (authenticator hardware manufacturers and the FIDO consortium), to which previous trust requirements (mainly service provider ones) has been delegated.
- We believe this new FIDO trust requirements map, puts too much power and responsibility in the hands of entities that cannot be trusted, especially in a world where online digital attacks are increasingly becoming state affairs.

Conclusion

- Trust requirements are associated with cost.

If anything in computer security *can* go wrong, it *will* eventually go wrong.

Are FIDO Trust Requirements worth it ?

To Whom?(Less liability for SPs)

References

- Ijlal Loutfi and Audun Jøsang. 1,2, pause: Lets start by meaningfully navigating the current
- online authentication solutions space. In *Trust Management IX*, volume 454 of *IFIP*
- *Advances in Information and Communication Technology*, pages 165–176. 2015.
- PandaLabs. PandaLabs Quarterly Report, Q2, June 2012.
- D. Prabhu andM. Adimoolam. Article: A novel dna based encrypted text compression. *IJCA*
- *Special Issue on Network Security and Cryptography*, NSC(2):36–41, December 2011.
- USDoD. *Trusted Computer System Evaluation Criteria*. US Department of Defence, 1985.
- Verizon. Control computer crime news. www.verizonenterprise.com/resources, 2013.
- *www.rsaconference.com/writable/.../arch-r07-scalable-**authentication**.**pdf***

Thank you for your attention