New Trends – New Threats – New Services in CyberSecurity

Teodor Cimpoesu, Director BU CyberSecurity

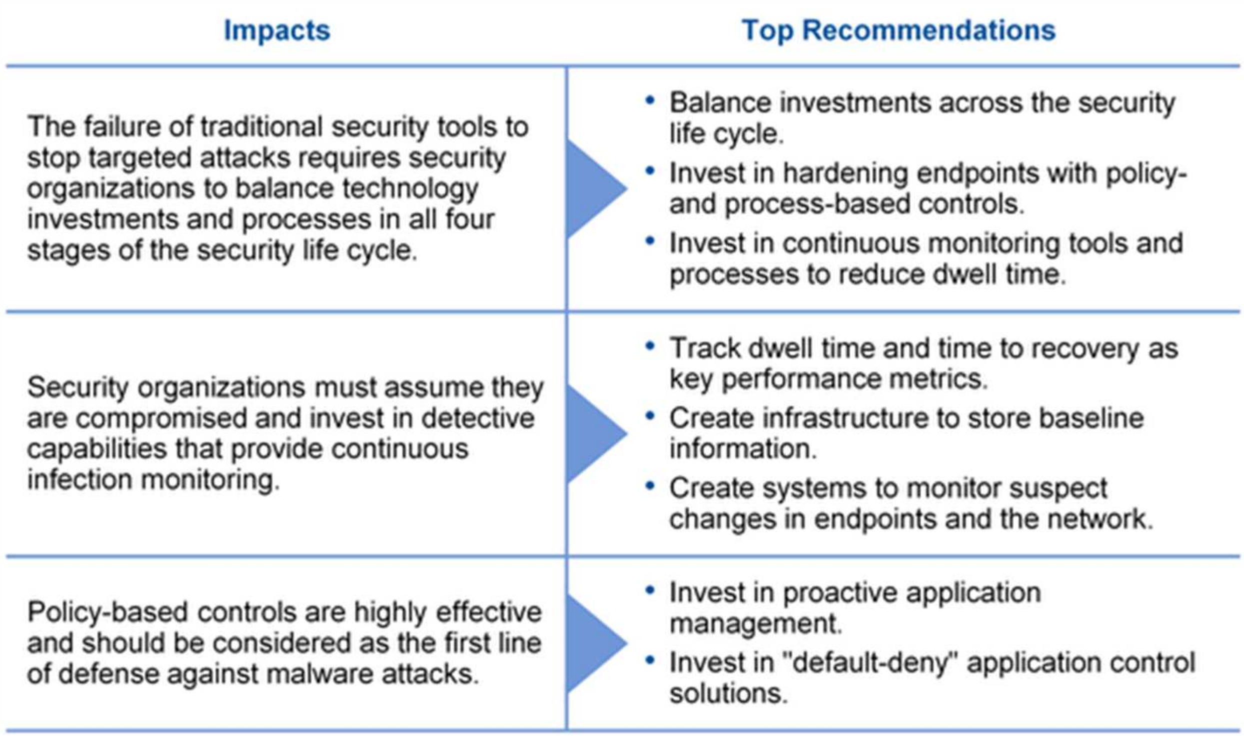
certSIGN

It is estimated that the future of this globally connected cyber world will include the following trends:

- The Internet will continue to be a fundamental element of the business mindset
- Flexible working practices facilitated by the explosion of mobile devices will be a basic lifestyle option
- The effective use of Internet, cloud computing and big data will enable business and mankind to further leverage the global wisdom of men and machines
- The increase in globalization of cyber relation will generate new risks that will have to be addressed based on the realities of our world.

Today

“There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don’t know it” – Gartner Inc. (2012)



Impacts	Top Recommendations
The failure of traditional security tools to stop targeted attacks requires security organizations to balance technology investments and processes in all four stages of the security life cycle.	• Balance investments across the security life cycle. • Invest in hardening endpoints with policy- and process-based controls. • Invest in continuous monitoring tools and processes to reduce dwell time.
Security organizations must assume they are compromised and invest in detective capabilities that provide continuous infection monitoring.	• Track dwell time and time to recovery as key performance metrics. • Create infrastructure to store baseline information. • Create systems to monitor suspect changes in endpoints and the network.
Policy-based controls are highly effective and should be considered as the first line of defense against malware attacks.	• Invest in proactive application management. • Invest in "default-deny" application control solutions.

Source: Gartner whitepaper, *“Malware Is Already Inside Your Organization; Deal With It”* (2014)

Why use Managed Security Services

1 **Fast track** to legal/regulatory compliance and **risk management**

2 **Import** of **skills** and capabilities – a dedicated tiger team to intervene

3 **Focus** your IT resources on support for **core functions** and competencies

4 **Visibility** - understand what happens, why, and what can you do about it.

5 **Actionability** – operations and data driven intelligence, for better decisions

6 **Smarter investment** – all those technologies are yours, as a service

What we do

certSIGN®
BY UTI

Technology Solutions

-

Complete cyber defenses projects

-

Cisco, Juniper, FireEye, IBM, Symantec, Websense, SkyBox, Microsoft, BAE Systems, Rapid7 and others.

MSSP Portfolio

-

Security Consulting
Audit & Pentest
Security Management
Managed Network Security
Managed Endpoint Security
Network Security Monitoring

UTI CERT

-

Incident Response
Data Forensics
Malware analysis & more

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT
AUTHORIZED TO USE CERT™
Software Engineering Institute
Carnegie Mellon

UTI ACADEMY

Training: EC-Council, (ISC)², ISACA, Mile2, Mandiant, CompTIA
+ Microsoft, Cisco, Fortinet and others.

CSIRT Services

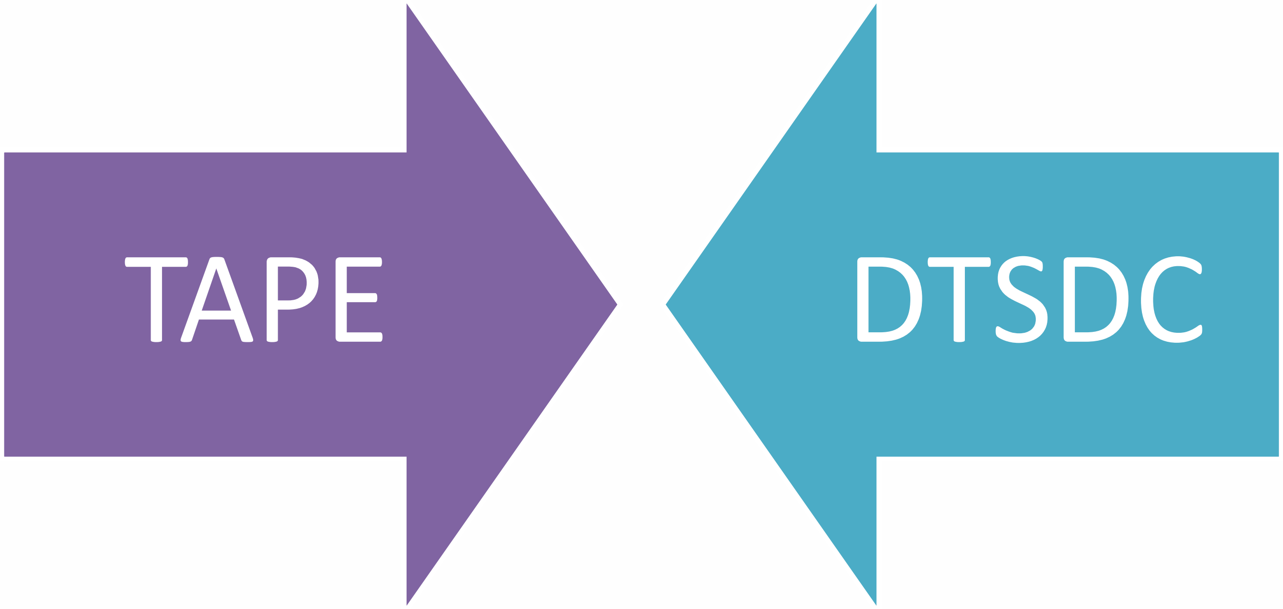
Security Management
Risk Analysis
Security Consulting
Security Validation
Education/Training
BC & DR Plans

Proactive Services
Announcements
Technology Watch
Configuration Management
Network Security Management
Intrusion Detection Services
Security Tools Development
Security Analytics

Reactive Services
Alerts and warnings
Incident Handling
Incident analysis
IR on site, support, coordination
Vulnerability Handling
Vuln analysis
Vuln response, coordination
Data Forensics
Artifact analysis
DF response, coordination

Research

certSIGN already managed to include in its services mechanisms developed from two major research projects:



TAPE

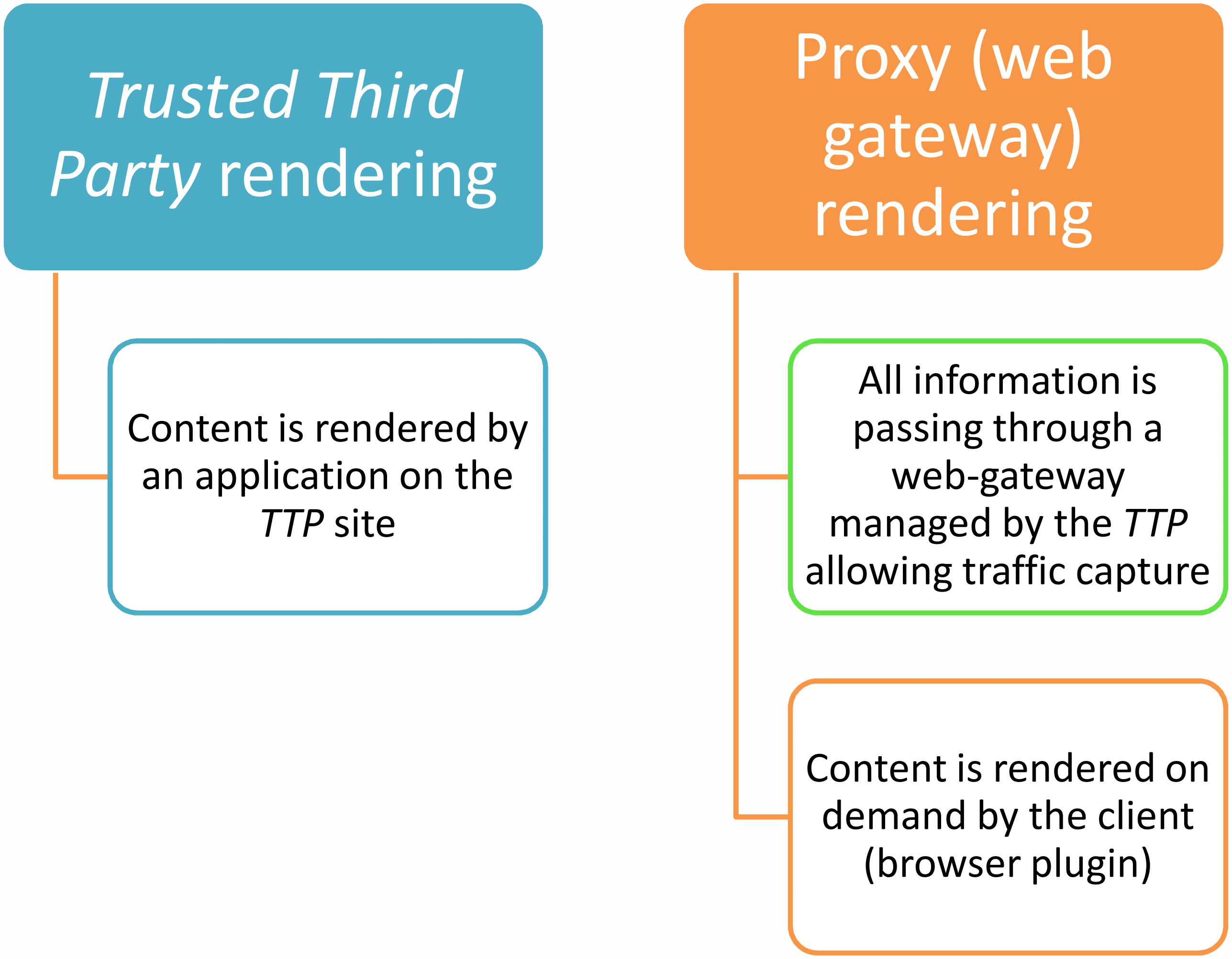
DTSDC

TAPE - Technologies for processing and assuring electronic content

CONTEXT

- Third Trusted Party service aiming:
  - **Guaranteeing the web-content**
    - Web-content non-repudiation
    - Web-content authenticity
    - Web-content source certification
  - **Long-term archiving of the web content**
    - Collecting and archiving the web-content
    - Preservation of content integrity
    - Long-term availability (keeping of the original presentation form)
  - **Usage of advanced security techniques**
    - EU ETSI's advanced signatures (CAdES-A)
    - Time-stamps from secured Trusted Timestamping Authorities (TTAs)
    - Secure archiving mechanisms (Trusted Archive Protocol)

Two scenarios



Trusted Third Party rendering

Content is rendered by an application on the *TTP* site

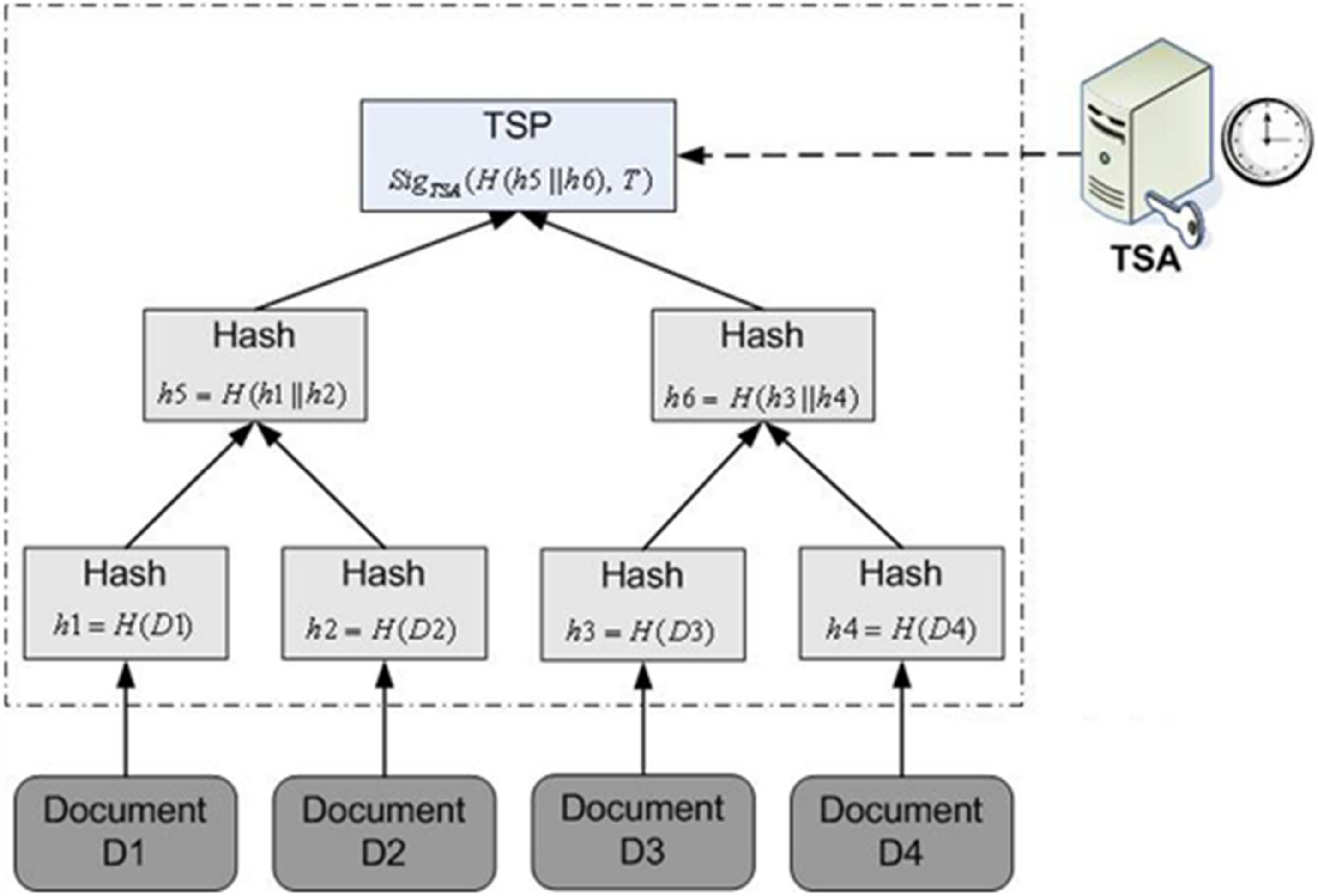
Proxy (web gateway) rendering

All information is passing through a web-gateway managed by the *TTP* allowing traffic capture

Content is rendered on demand by the client (browser plugin)

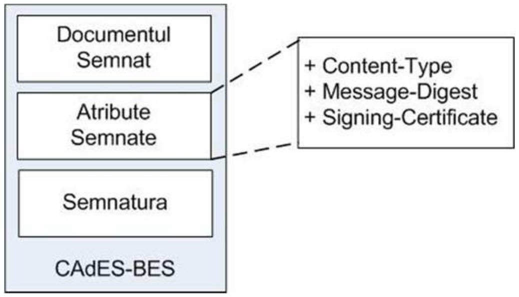
Security mechanisms

- Hash-trees and Timestamping: ensuring integrity

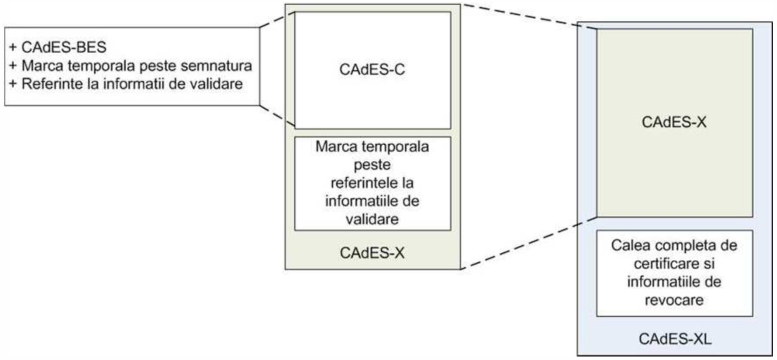


Security mechanisms (cont.)

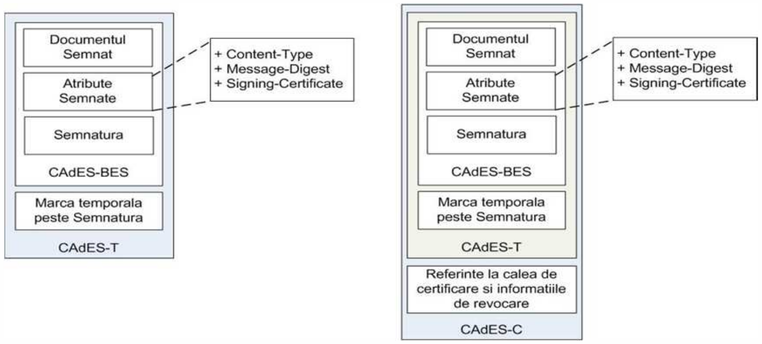
- Advanced signatures: long-times security



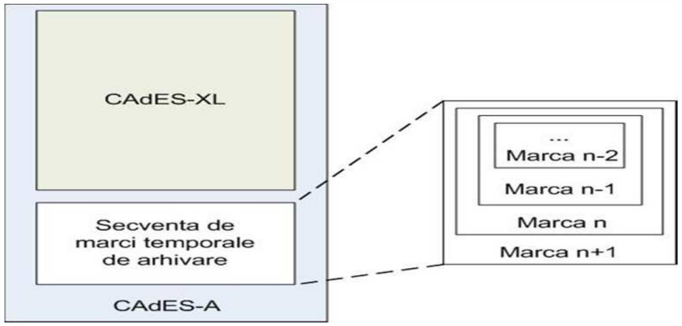
CAdES-BES


+ CAdES-BES
+ Marca temporala peste semnatura
+ Referinte la informatii de validare
CAdES-C
Marca temporala peste referintele la informatiile de validare
CAdES-X
CAdES-X
Calea completa de certificare si informatiile de revocare
CAdES-XL

CAdES-X, CAdES-XL



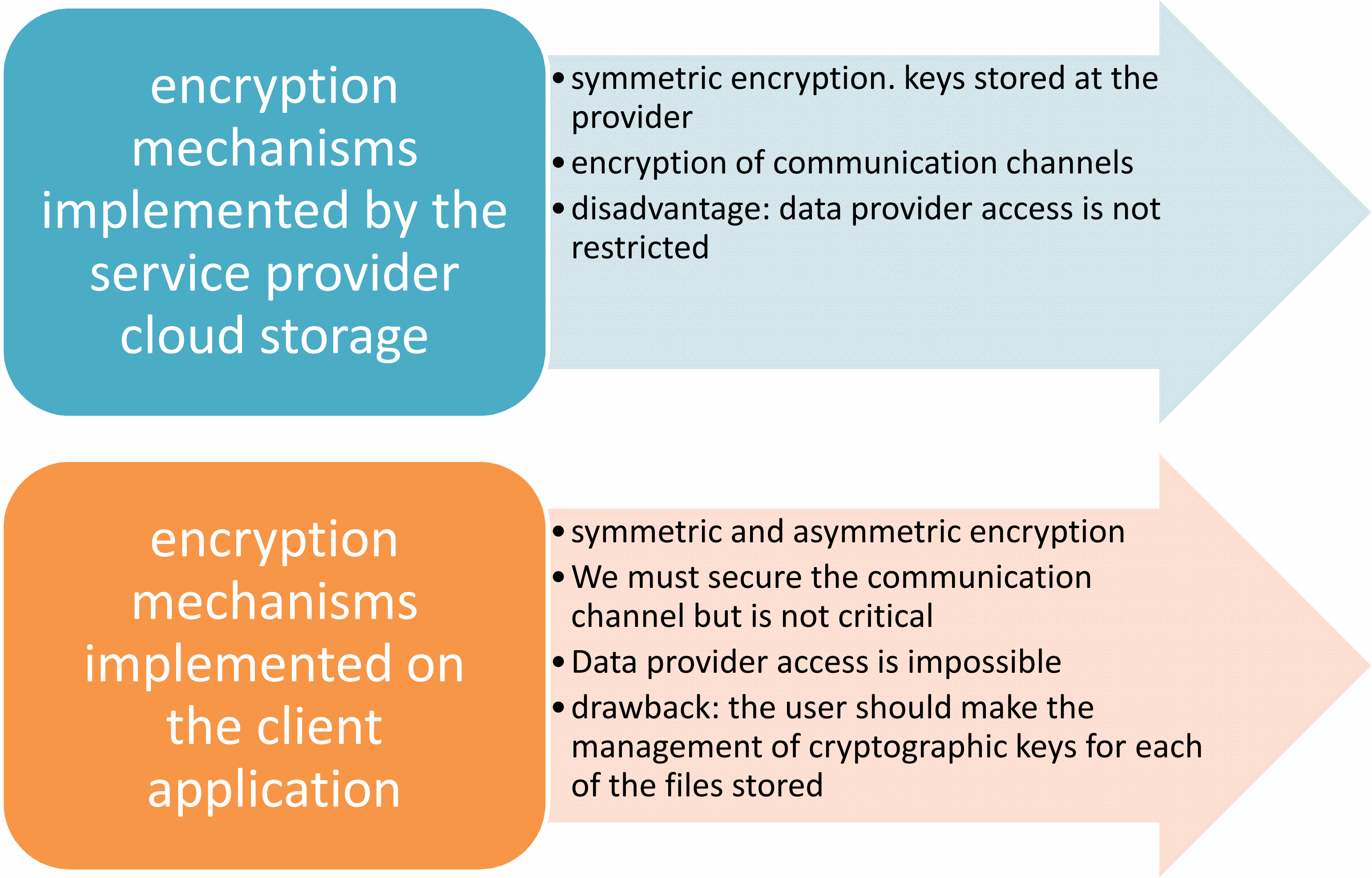
CAdES-T, CAdES-C



CAdES-A

DTSDC - Technologies to protect information stored in cloud

Protecting stored data. Current situation



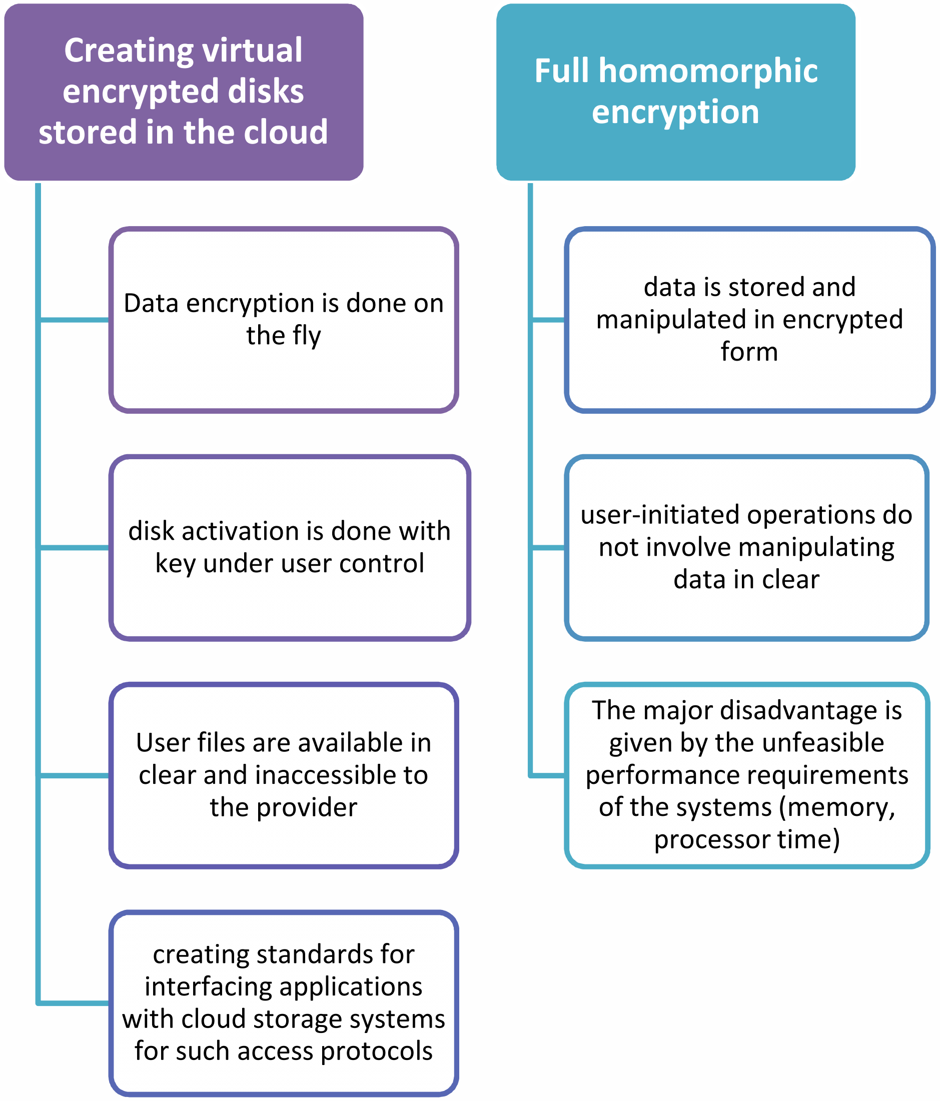
encryption mechanisms implemented by the service provider cloud storage

- symmetric encryption. keys stored at the provider
- encryption of communication channels
- disadvantage: data provider access is not restricted

encryption mechanisms implemented on the client application

- symmetric and asymmetric encryption
- We must secure the communication channel but is not critical
- Data provider access is impossible
- drawback: the user should make the management of cryptographic keys for each of the files stored

Technology development directions



Creating virtual encrypted disks stored in the cloud

- Data encryption is done on the fly
- disk activation is done with key under user control
- User files are available in clear and inaccessible to the provider
- creating standards for interfacing applications with cloud storage systems for such access protocols

Full homomorphic encryption

- data is stored and manipulated in encrypted form
- user-initiated operations do not involve manipulating data in clear
- The major disadvantage is given by the unfeasible performance requirements of the systems (memory, processor time)

Thank you.

certSIGN®
BY UTI

Teodor.Cimpoesu@certSIGN.ro
@cteodor, +40724.039.254
csirt@certsign.ro