



<u>Thème :</u>

Cipher Data Centric Security

<u>Présenté par :</u> Thierry Leblond, CEO & Co-fondateur SCILLE / PARSEC





Zero trust Data Centric Security :

What is this ?

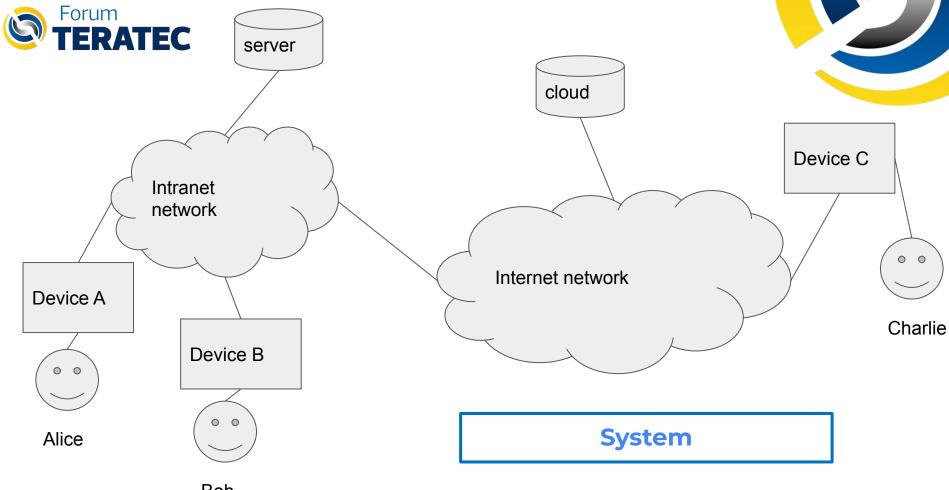


• Security is no longer an option:

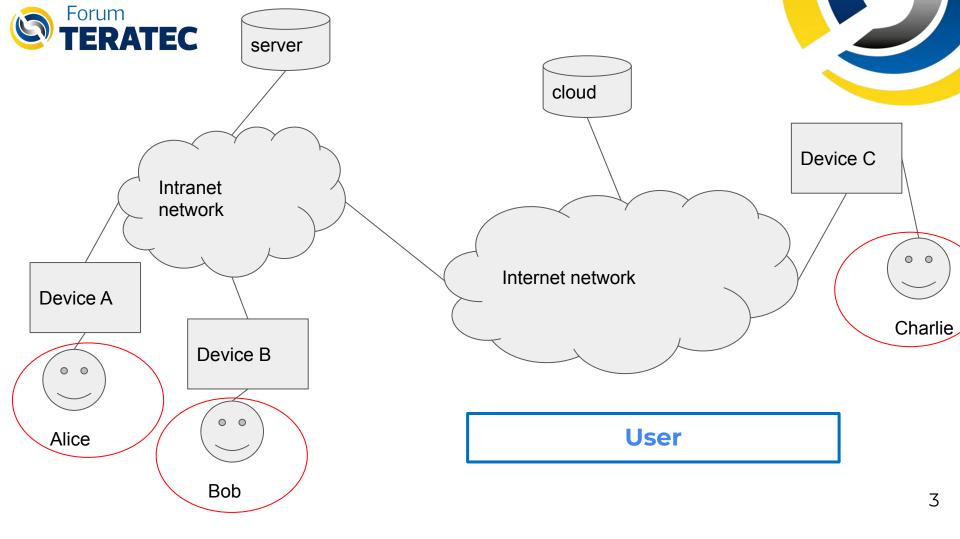
- Obsolescence of the perimeter security model
- NIS2 directive applicable end 2024
- Zero Trust DoD strategy / US NIST standards
- Nato DCS standardization
- Requirements
 - security as close as possible to the user
 - confidentiality, integrity, non-repudiation, authenticity, anonymization, traceability, historization, revocation

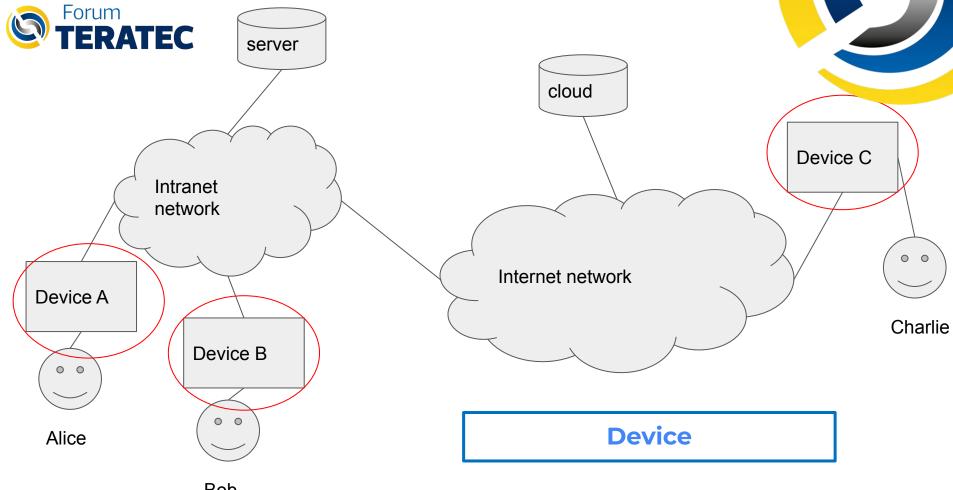
Means

- \circ Zero trust \Rightarrow systematic verification
- Zero knowledge \Rightarrow crypto implementation of "right to know".
- Data Centric Security ⇒ crypto-control of data & classification metadata



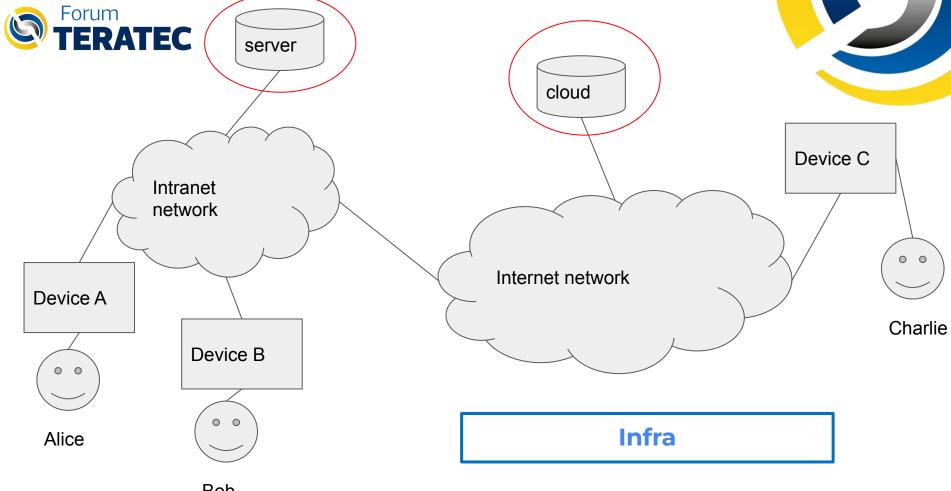
Bob

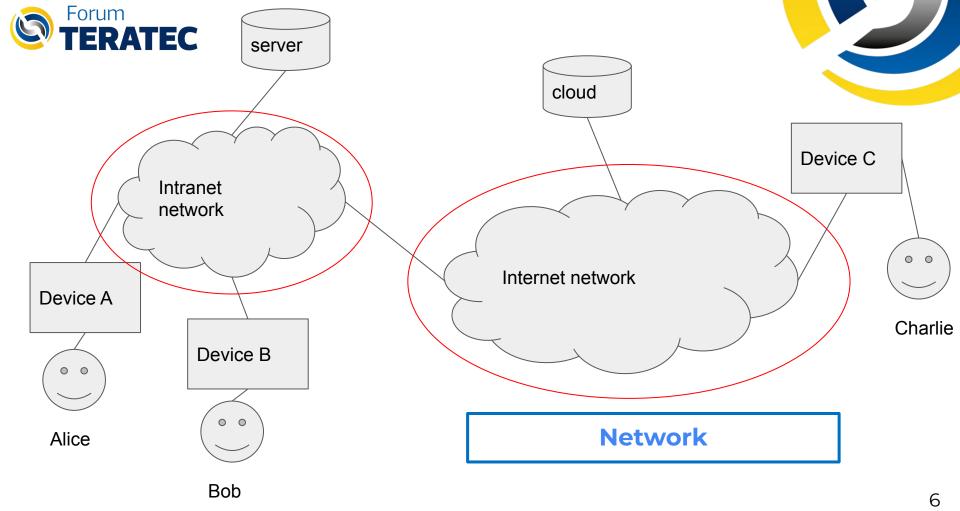


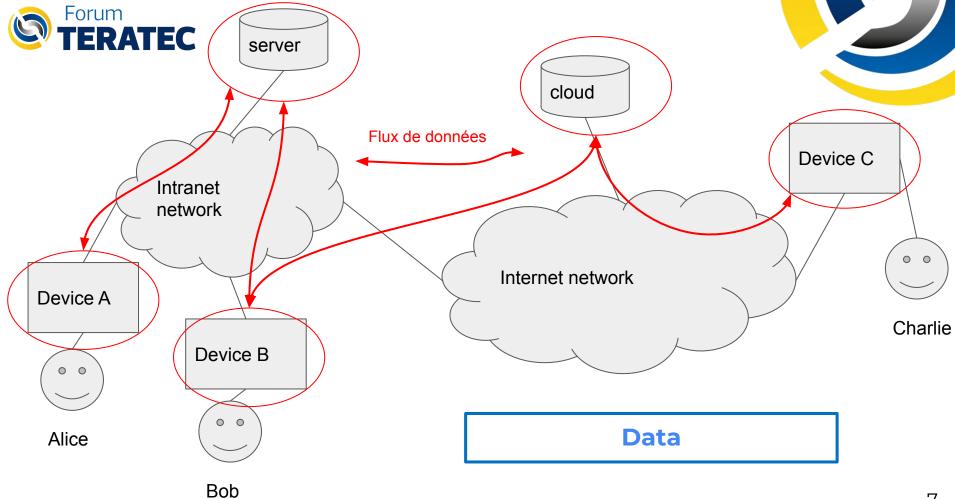


Bob

4





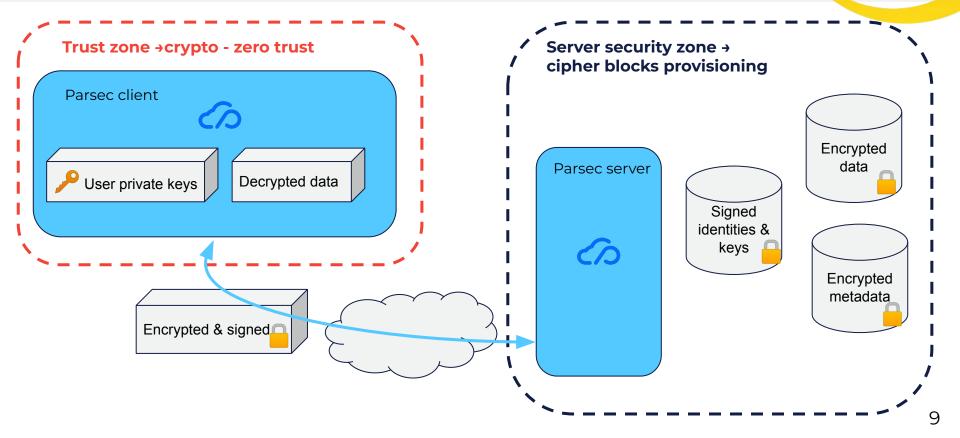


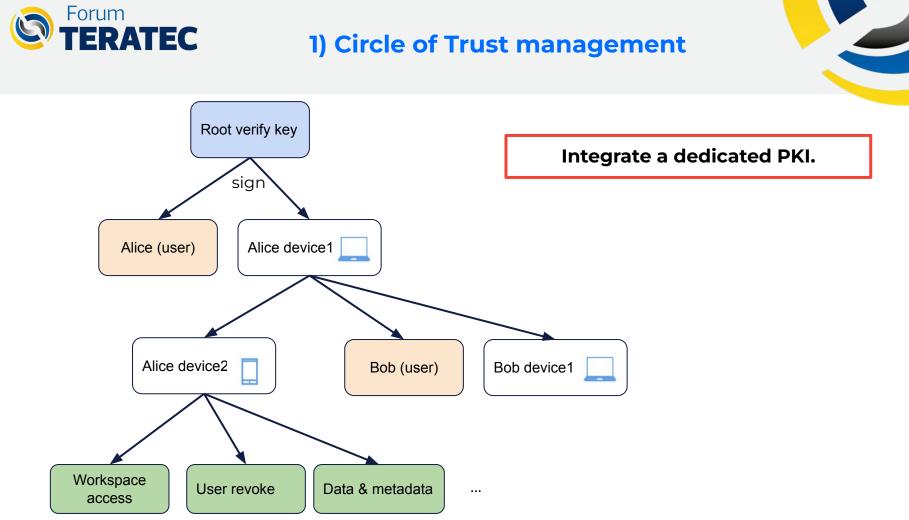


US DoD standard Zero Trust

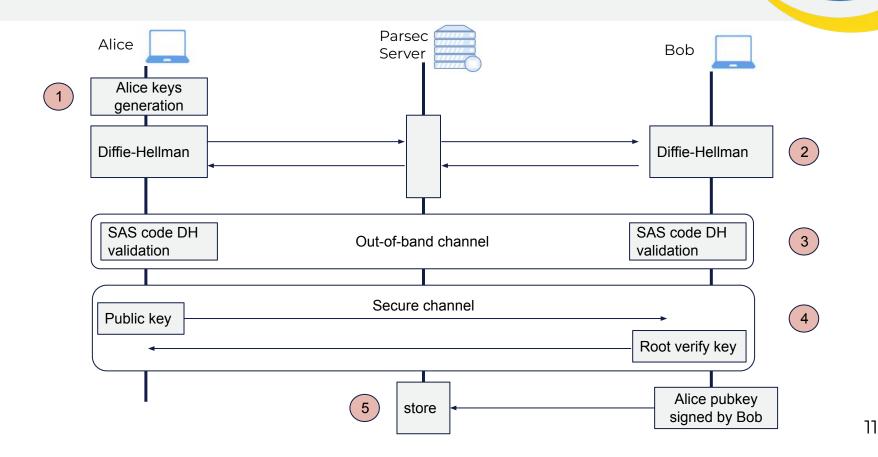
User	Device	Physical Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
I.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
I.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authorization with Real Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User and Entity Behavio Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption & Rights Management		6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response (EDR & XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Forum TERATEC Parsec: Systematic user-centric encryption





EVALUATE: Forum **TERATEC** 2) Simplified user enrollment & dedicated PKI



Forum TERATEC 2) Simplified user enrollment & dedicated PKI

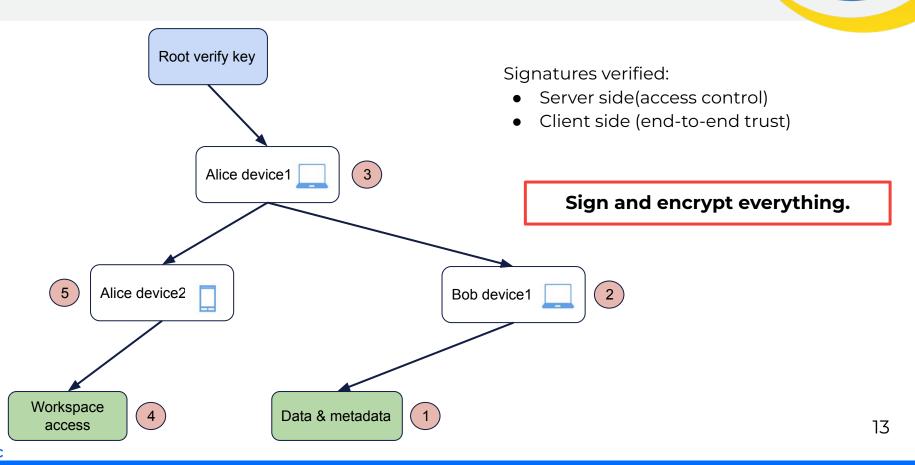
	arsec-vmp4	5	Ů + ©	••• • • < >	parsec.cloud	\$	0 + 0
 Gérer mon organisation 	Invitations en cours	۹ 🔹	Thomas Linere ~ Connecté •	< Gérer mon organisation	Invitations en cours	۹ ک	Thomas Linere V Connecte •
# Utilisateurs	≰ Inviter un utilisateur		III III liste	# Utilisateurs	🛓 Inviter un utilisateur	_	📰 🖽 liste
Actifs Révoqués Invitations en cours	Code admin. Code invité Coordannées	O X		Actifs Révoqués Invitations en cours. @	Conde invité Coordinnées	-O X	
Espaces de travail Stockage Facturation	Partage du code admin Veuillez communiquer le code ci-dessous à l'utilis	sateur invité.	Refuser	 Espaces de travail Stockage Facturation 	Réception du code invité Cliquez sur le code que vous donne l'invité.		Refuser
	ERTS				ERTS UREE © DSDS HEZG		
	(En attente de l'invité)	D.			Aucun de ces cades		
-9							
	20	léments			2 élérne	nts	

Only humans creates trust.

https://drive.google.com/file/d/1_abgGYTzRJwuTshZDQ0JMGnwb5_Opqyt/edit

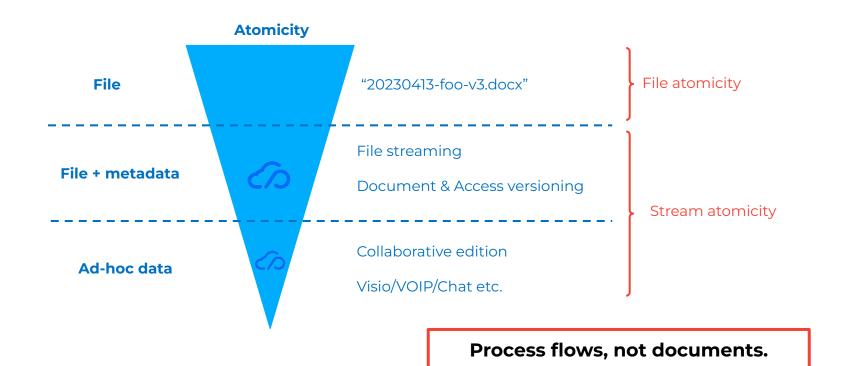


3) Zero-trust data access





4) File versus stream atomicity





5) Challenge 1 : Backward compatibility



In a classic web application:

- update functionalities → evolve the data model
- very simple on a centralized database

In an approach that no longer trusts the central server:

- All data is signed and encrypted, and the central server sees nothing (we don't trust it).
- How do you add a new concept (e.g., adding backward-compatible data classification)?
 - o at server level
 - at client level: who signs?

<u>Challenge n°1</u>: the end-to-end encryption issue exacerbates the resolution of data backward compatibility.



6) *Challenge 2:* Strong applicative security integration

In a classic web application:

- security layer: TLS
- application layer: REST API

In a Data Centric Security application :

- REST API with signed & encrypted data
- Use case: Synchronization of (large!) Parsec files
 - divide file data into blocks
 - upload encrypted blocks to Parsec server
 - create a file manifest to reconstruct a given version of the file
 - o file manifest signed and encrypted (with workspace key), uploaded to Parsec server
 - ⇒ problematic: user access revocation (file manifest re-encryption without signature change)
 - → upload order between blocks and file manifest

<u>Challenge n°2</u>: strong integration between security and applications.



7) Eventual consistancy



In a classic web application:

- he client is seen as the graphical interface
- a request to the server is enough to modify system state

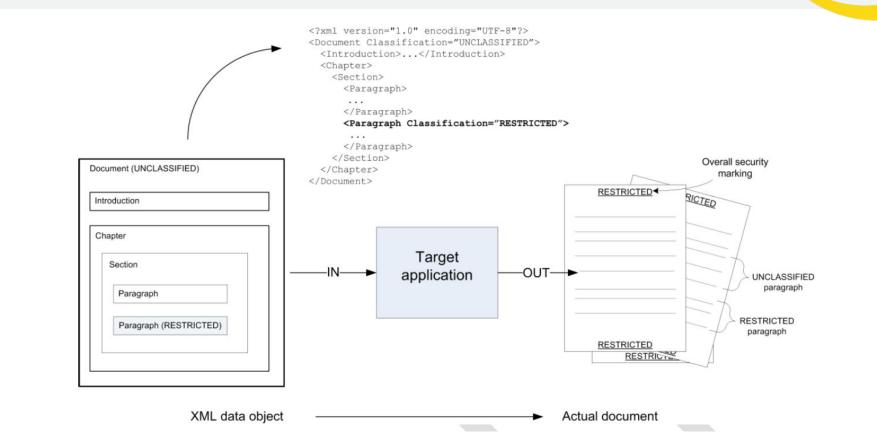
In a PARSEC logic, client and server states must be reconciled

- Issue 1) = withstand network failure
 - survive loss of connection
- Issue 2) = tolerate network latency and manage time scales
 - constant de-correlation between server state and client state
 - local modification must remain instantaneous as seen by the user
- Consequence: asynchronous operating mode:
 - operations are always performed locally
 - network outages have no consequences
 - client and server systems accept the decollation and agree when the network connection is re-established

<u>Challenge n°3</u>: correlate server and client status despite latency and network interruptions.



DCS NATO vision of data labelling



18



DCS NATO maturity levels

- DCS#1: Labeling
- DCS#2 : Trusted binding (label signature))
- DCS#3 : Signed and ciphered data & metada ta

