Access Control Mechanisms Analysis for a Dynamic and Decentralized Approach of Data-Centric Security (DCS)

C&ESAR'24: Computer & Electronics Security Application Rendezvous, Nov. 20-21, 2024, Rennes, France

Etienne Lemonnier
Académie Militaire de Saint-Cyr Coëtquidan
CReC Saint-Cyr

Jamal El Hachem
Université Bretagne Sud
IRISA

Lionel Touseau
Académie Militaire de Saint-Cyr Coëtquidan
CReC Saint-Cyr

Jérémy Buisson
École de l'Air et de l'Espace
CRéA

Nicolas Belloir
Académie Militaire de Saint-Cyr Coëtquidan
CReC Saint-Cyr

Jean-François Wiorek
Thales Group

CHAIRE DE CYBERDÉFENSE ET CYBERSECURITÉ

THALES

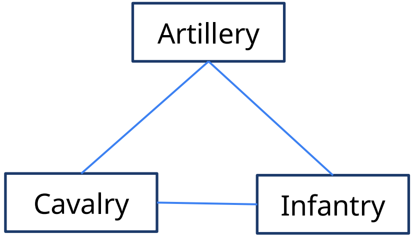
Data in collaborative combat

Sensitive data is exchanged

Classification and need-to-know

Scales of interoperability

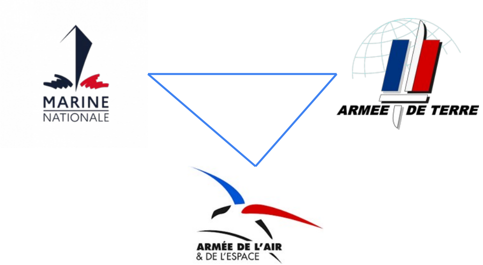
https://theatrum-belli.com/les-technologies-du-combat-collaboratif-un-enjeu-majeur-chez-thales-pour-accompagner-nos-forces-armees/

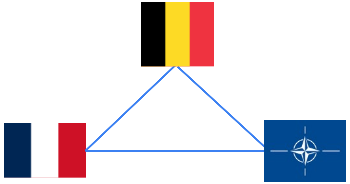


Artillery

Cavalry

Infantry





Outline

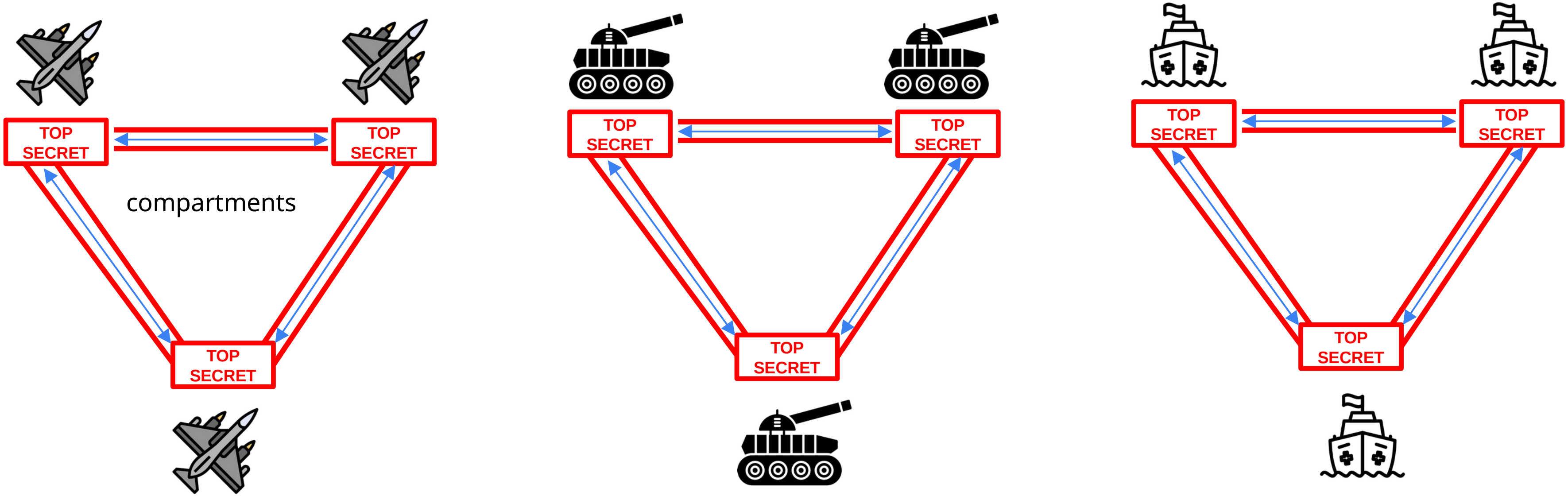
Data-centric security (DCS): approach

DCS in collaborative combat: example and limitations

Access control mechanisms that answers the limitations

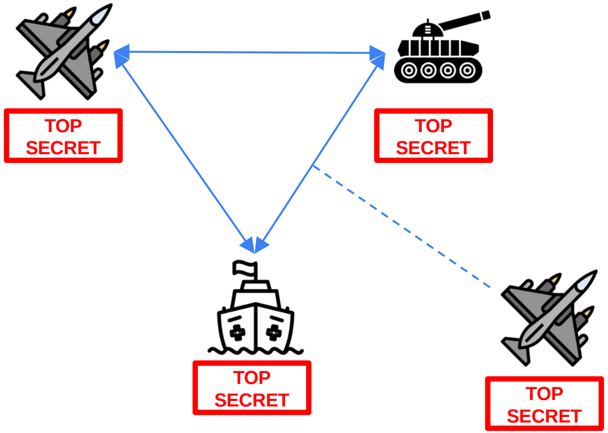
Compartmentalized networks

Expensive and not interoperable



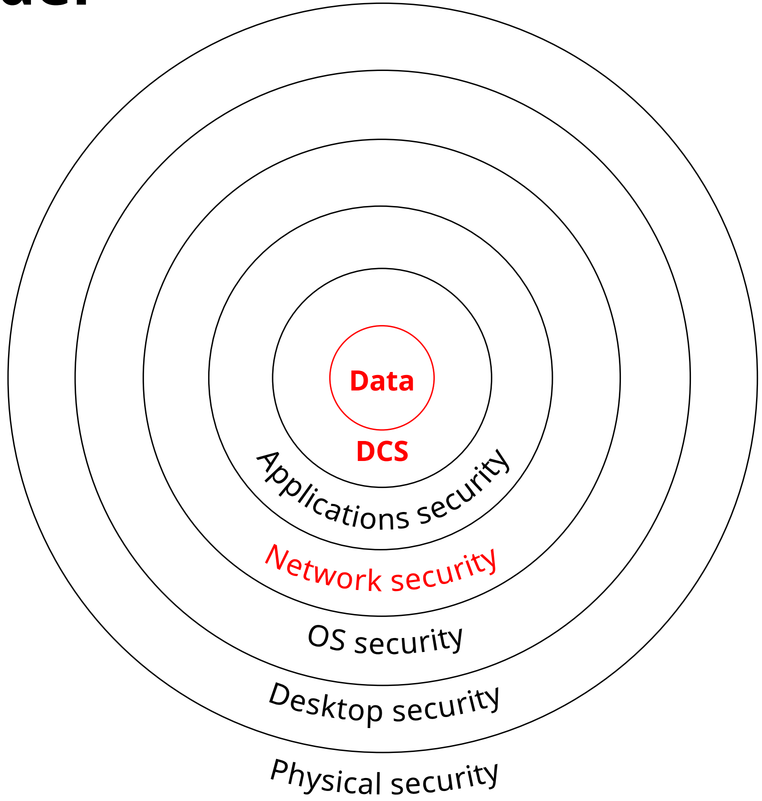
Non-compartmentalized networks

Available everywhere **but** not secure



Opportunity effect

Security onion model



→ Circles are not exclusive

Data-centric security (DCS)

Focusing security on data itself instead of networks or applications security

Security will have the same lifespan as data and will be applied at the three states of data

Avoid recipient listing

Security will not depend on where the data is stored or transmitted

NATO standard:

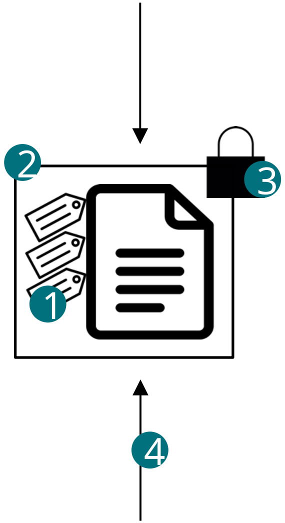
- STANAG-4774 (2017): “The NATO mission environment is evolving from network-centric based security architecture to Data-Centric based security architecture”

NATO Standardization Office (NSO), Allied data processing publication 4774 (ADatP4774) : Confidentiality Metadata Label Syntax, Technical Report Edition A Version 1, North Atlantic Treaty Organization, 20 December 2017.

How to DCS ?

→ Four properties:

1) Labelling of documents: classification, protection label, metadata
2) Formatting: interoperability (STANAG-4778)
3) Cryptographic protection and signature
4) Context and trust

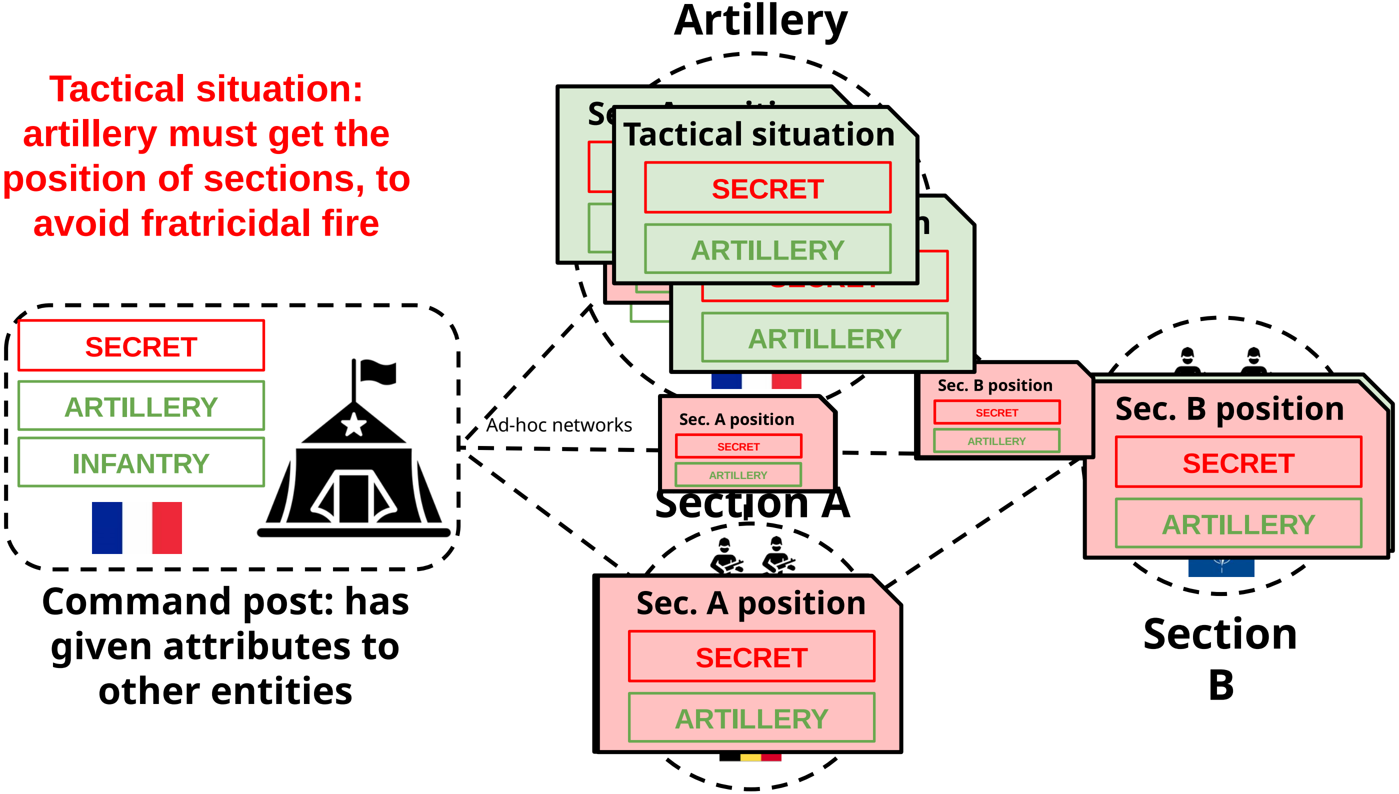


Penders, Ate, Max Van Der Horst, Alex Van Der Linden, Maurits De Graaf, Thomas Quillinan, et Gregor Pavlin. « A Secure Information Management and Interoperability Framework: Enabling Distributed Fusion Engines for Military IoT Applications ». In 2024 International
NATO Standardization Office (NSO), Standardization Agreement 4778 (STANAG-4778) :Metadata binding mechanism, Technical Report NSO/1328(2018)CAP1/4778, North AtlanticTreaty Organization, 26 October 2018.

Pictograms : Freepik

DCS example from the collaborative combat domain

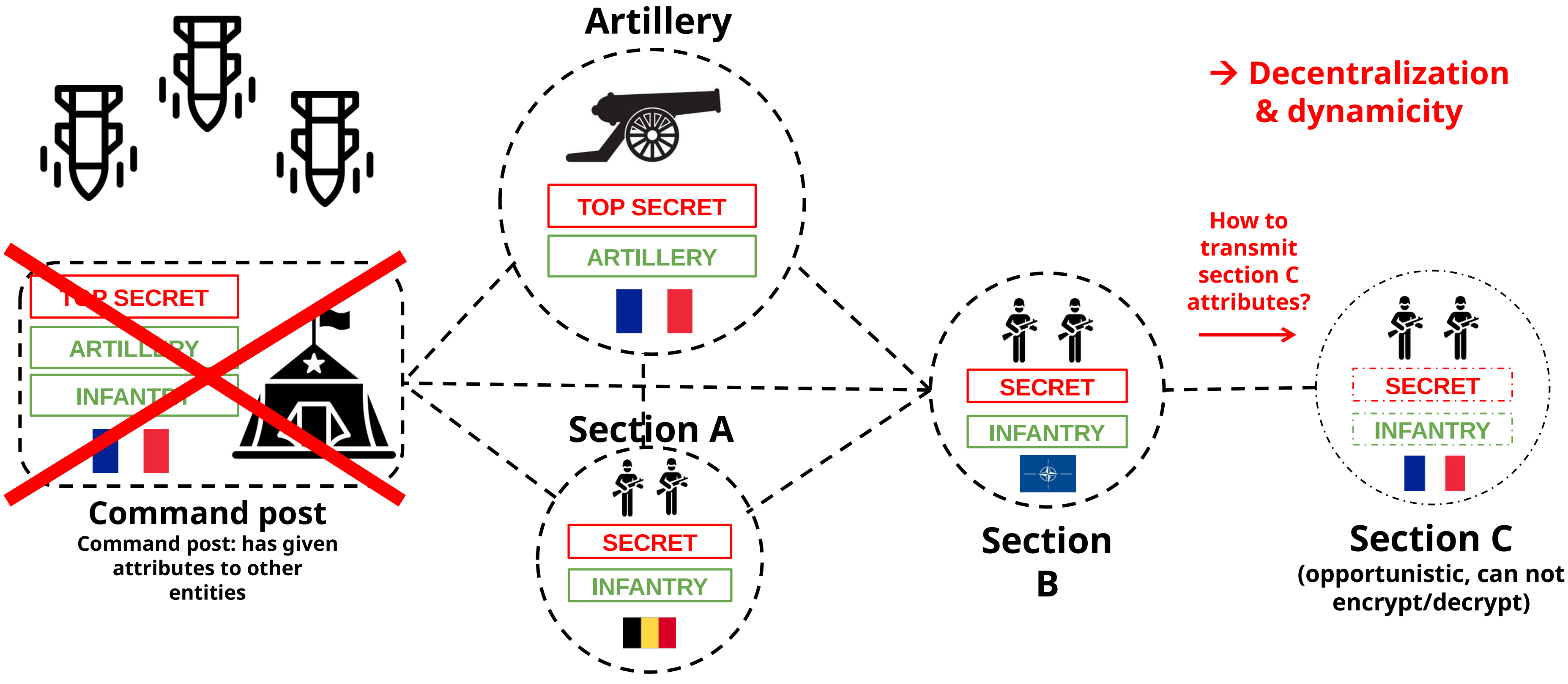
Tactical situation: artillery must get the position of sections, to avoid fratricidal fire



Command post: has given attributes to other entities

Pictograms : Freepik

Limitations of DCS centralized approaches



→ Decentralization & dynamicity

DCS challenges

Needed security properties in access control mechanisms:

Decentralization: each actor must still be able to generate access rights for another actor.
Permits:

- Availability
- Actor redundancy (avoid single point of failure)
- Scalability

Dynamicity: each actor must be authorized to join or leave the secure system, without giving all accesses at the beginning (users can gain or lose accesses)

Objective: DCS implementation + decentralization + dynamicity

To answer DCS objectives…

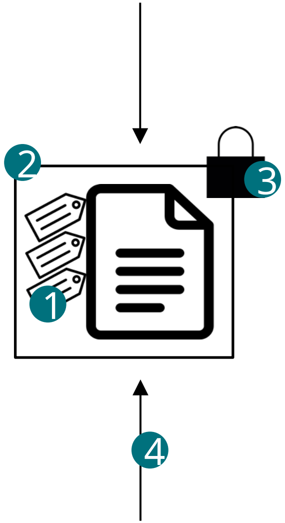
1) Labelling of documents: classification, protection label, metadata

2) Formatting: interoperability (STANAG-4778)

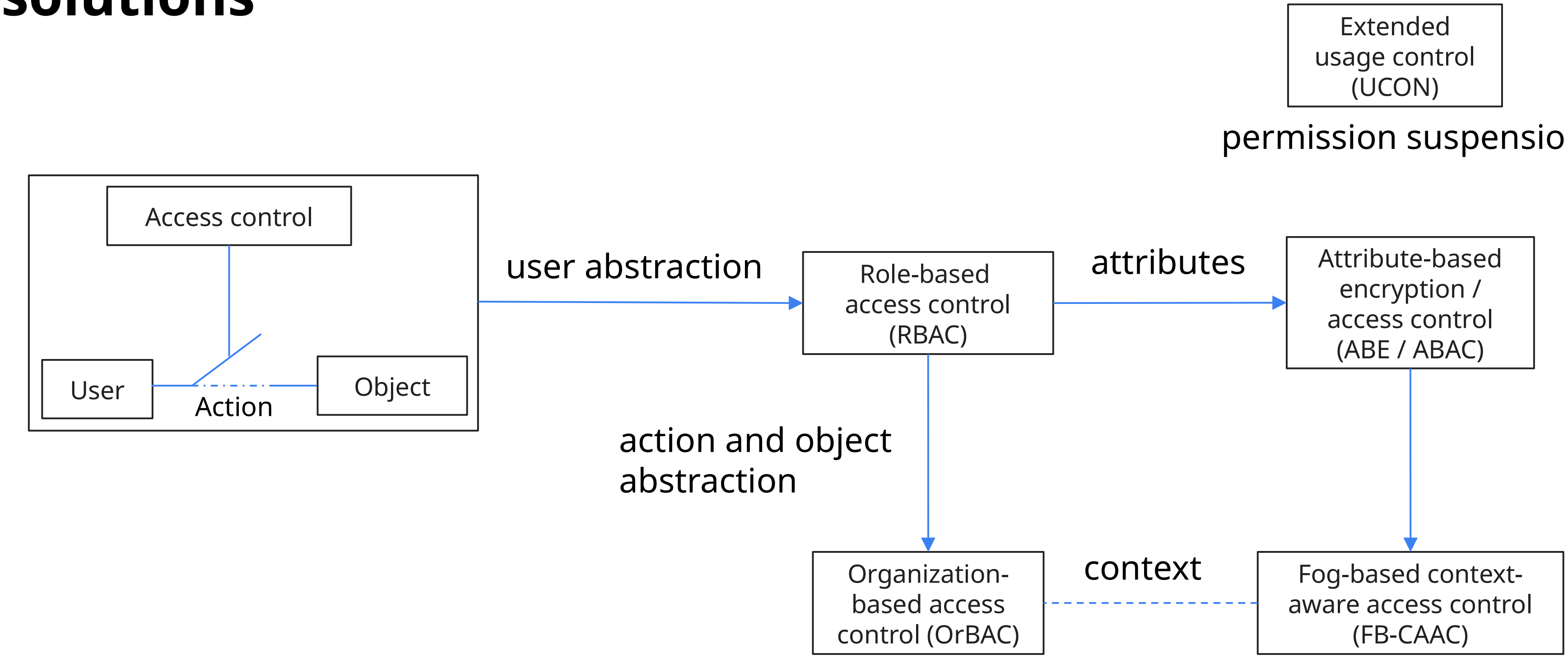
3) Cryptographic protection and signature

4) Context and trust

Access control mechanisms



Access control mechanisms to address solutions


Extended usage control (UCON)
permission suspension
Access control
User
Action
Object
user abstraction
Role-based access control (RBAC)
attributes
Attribute-based encryption / access control (ABE / ABAC)
action and object abstraction
Organization-based access control (OrBAC)
context
Fog-based context-aware access control (FB-CAAC)

Analysis of dynamic and decentralized access control mechanisms according to different criteria

Caption:

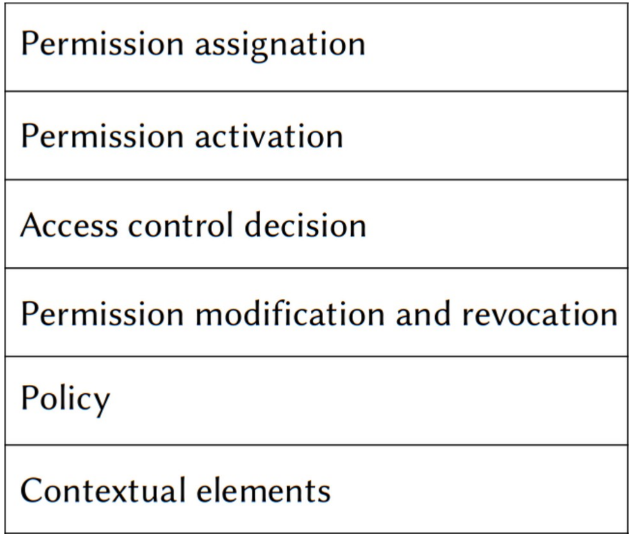
● The solution meets the criteria

○ The paper describes the criteria but not implement it

N/A Not applicable: no keys to encrypt/decrypt in access control models

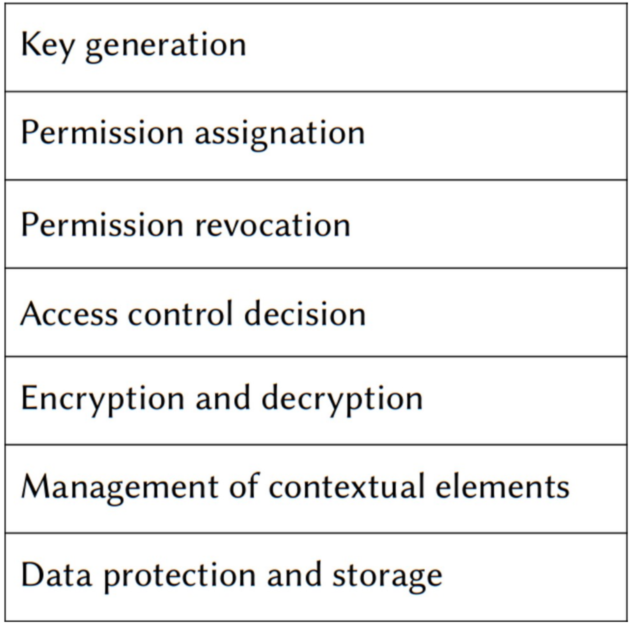
Empty: criteria is not addressed

dynamicity



Permission assignation
Permission activation
Access control decision
Permission modification and revocation
Policy
Contextual elements

decentralization



Key generation
Permission assignation
Permission revocation
Access control decision
Encryption and decryption
Management of contextual elements
Data protection and storage

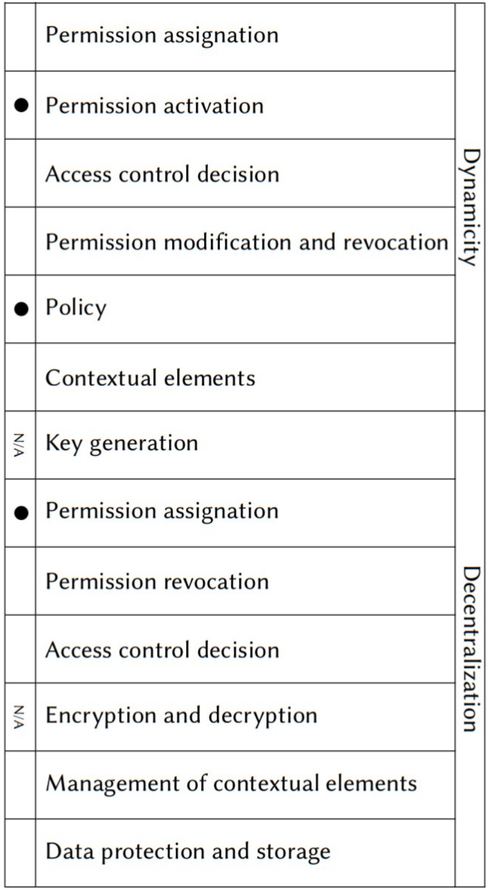
RBAC: role-based access control

Permissions are associated with roles, and users are assigned to appropriate roles

Each session is a dynamic mapping of one user to possibly many roles

Dynamic policy over its lifetime

Mutually exclusive roles



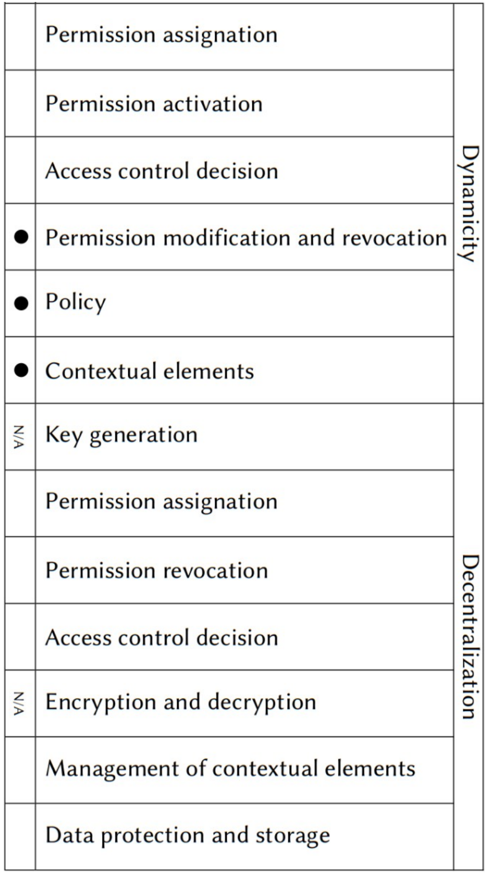
	Permission assignation	Dynamicity
●	Permission activation	
	Access control decision	
	Permission modification and revocation	
●	Policy	
	Contextual elements	
N/A	Key generation	Decentralization
●	Permission assignation	
	Permission revocation	
	Access control decision	
N/A	Encryption and decryption	
	Management of contextual elements	
	Data protection and storage	

R. S. Sandhu, Role-based access control, in: Advances in computers, volume 46, 1998, pp. 237–286. doi:10.1016/S0065-2458(08)60206-5.

OrBAC: organization-based access control

Abstracting « subject-action-object » to « role-activity-view » for organizations

Adds prohibitions, recommendations, obligations to permissions, with context

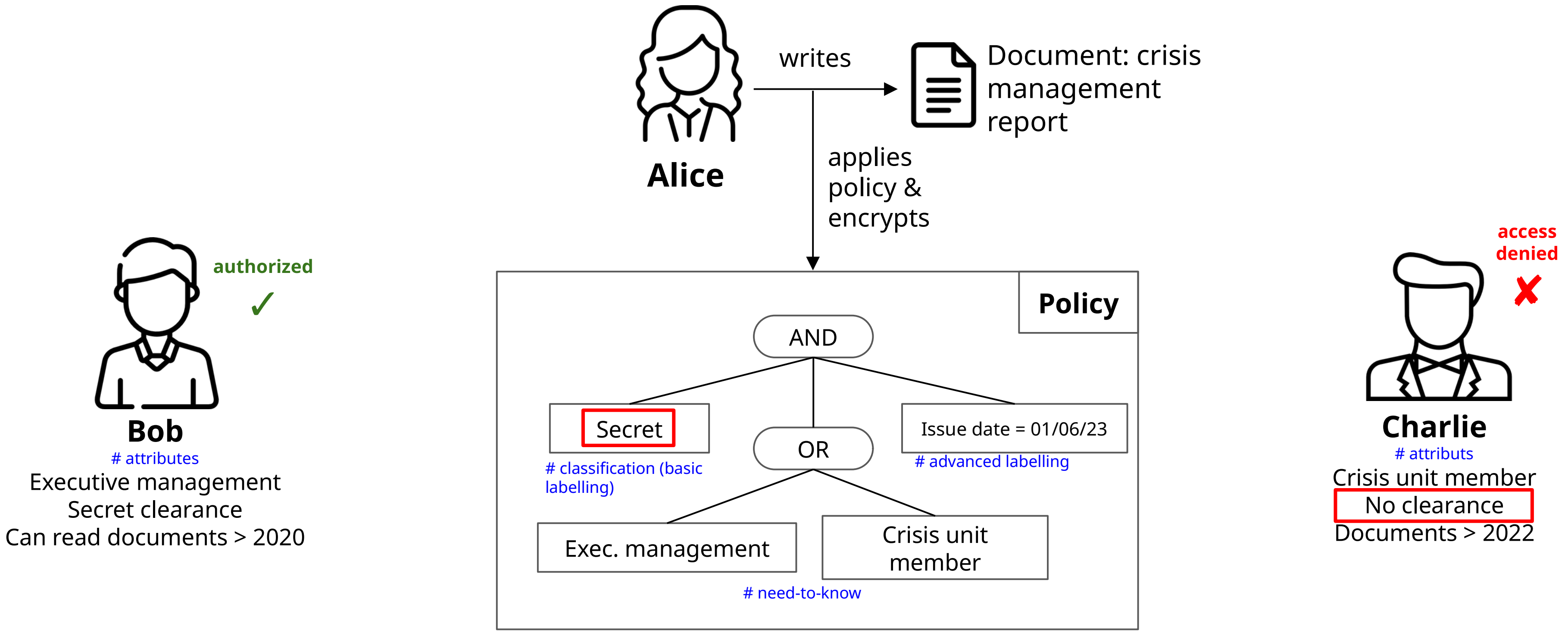


	Permission assignation	Dynamicity
	Permission activation	
	Access control decision	
●	Permission modification and revocation	
●	Policy	
●	Contextual elements	
N/A	Key generation	Decentralization
	Permission assignation	
	Permission revocation	
	Access control decision	
N/A	Encryption and decryption	
	Management of contextual elements	
	Data protection and storage	

A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, G. Trouessin, Orbac: un modèle de contrôle d'accès basé sur les organisations, Cahiers francophones de la recherche en sécurité de l'information 2 (2003) 30–40.

Pictograms : Freepik

Attribute-based access control (ABAC)



Alice

writes

Document: crisis management report

applies policy & encrypts

Policy

AND

Secret

# classification (basic labelling)

OR

Issue date = 01/06/23

# advanced labelling

Exec. management

Crisis unit member

# need-to-know

Bob

authorized ✓

# attributes

Executive management

Secret clearance

Can read documents > 2020

Charlie

access denied ✘

# attributs

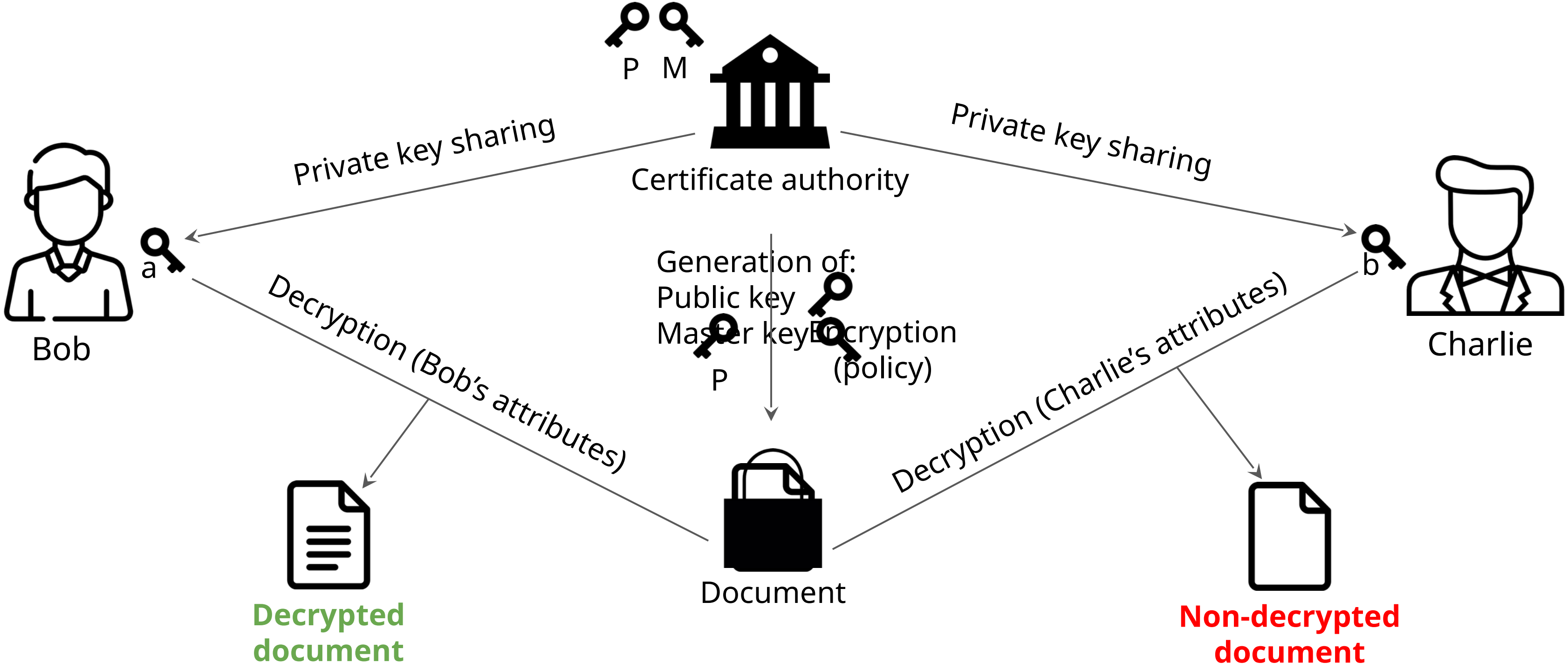
Crisis unit member

No clearance

Documents > 2022

Pictograms : Freepik

Ciphertext-policy attribute-based encryption (CP-ABE)



J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Symposium on security and privacy, 2007, pp. 321–334. doi:10.1109/SP.2007.11.

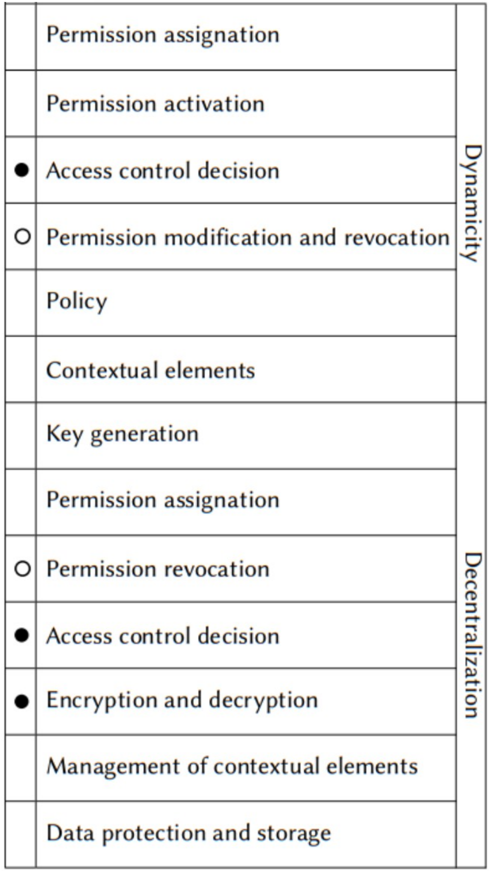
CP-ABE: ciphertext-policy attribute-based encryption

Embeds the access policy in the ciphertext, as well as user attributes in their keys

When the keys are distributed, system becomes autonomous

Revocation: appending expiration date to attributes

Variant: DMA-ABE with multi authorities



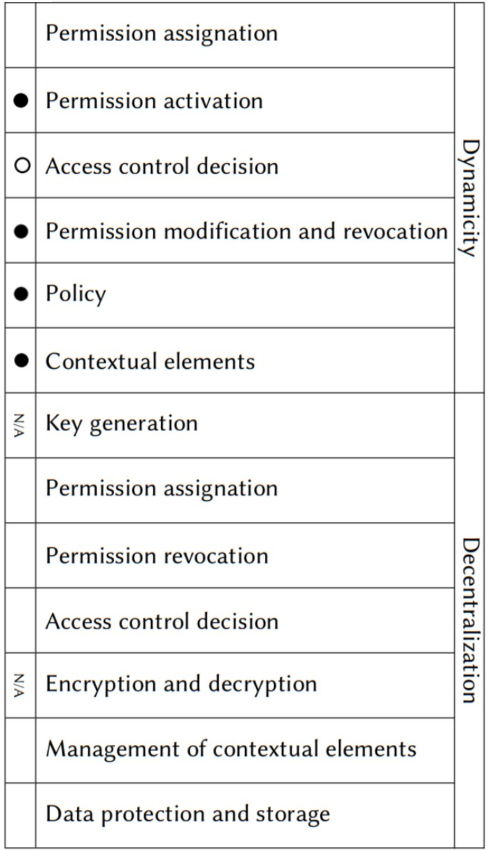
	Permission assignation	Dynamicity
	Permission activation	
●	Access control decision	
○	Permission modification and revocation	
	Policy	
	Contextual elements	
	Key generation	Decentralization
	Permission assignation	
○	Permission revocation	
●	Access control decision	
●	Encryption and decryption	
	Management of contextual elements	
	Data protection and storage	

J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Symposium on security and privacy, 2007, pp. 321–334. doi:10.1109/SP.2007.11.

FB-CAAC: fog-based context-aware access control

Access control adapted for IoTs

Introduces a taxonomy that defines context categories in access control: location, temporality, user, object, environment



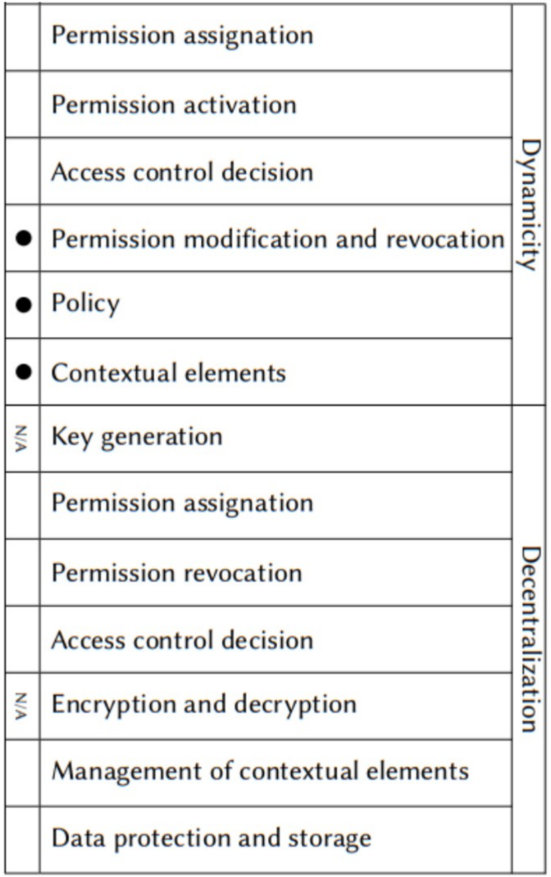
	Permission assignation	Dynamicity
●	Permission activation	
○	Access control decision	
●	Permission modification and revocation	
●	Policy	
●	Contextual elements	
N/A	Key generation	Decentralization
	Permission assignation	
	Permission revocation	
	Access control decision	
N/A	Encryption and decryption	
	Management of contextual elements	
	Data protection and storage	

A. Kayes, R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha, I. Kumara, A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues, Sensors (2020) 2464. doi:10.3390/ s20092464.

Extended UCON: usage control

Adapts UCON model to complex and dynamic environments

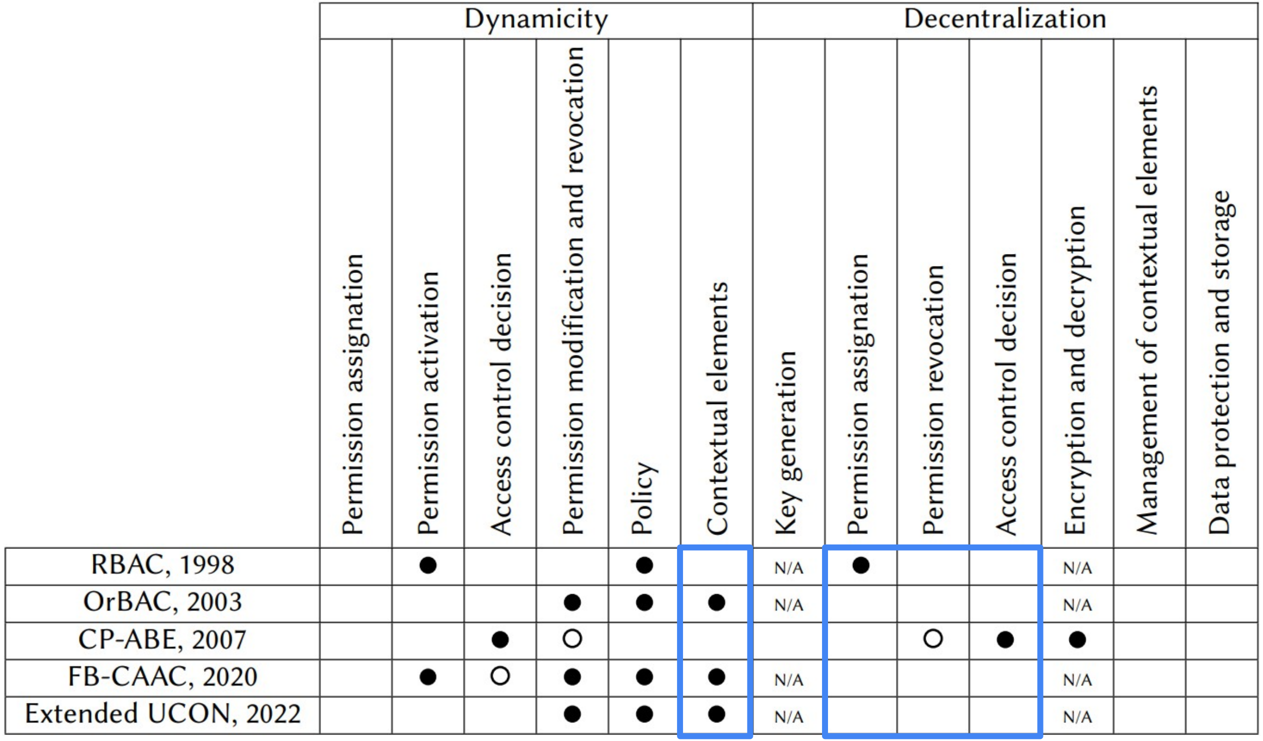
A deterministic finite automaton defines the new authorization lifecycle



	Permission assignation	Dynamicity
	Permission activation	
	Access control decision	
●	Permission modification and revocation	
●	Policy	
●	Contextual elements	
N/A	Key generation	Decentralization
	Permission assignation	
	Permission revocation	
	Access control decision	
N/A	Encryption and decryption	
	Management of contextual elements	
	Data protection and storage	

A. Hariri, A. Ibrahim, T. Dimitrakos, B. Crispo, Wip: Metamodel for continuous authorisation and usage control, in: Proceedings of the 27th ACM Symposium on Access Control Models and Technologies, 2022, pp. 43–48. doi:10.1145/3532105.3535039.

Analysis of dynamic and decentralized access control mechanisms according to different criteria



	Dynamicity						Decentralization						
	Permission assignation	Permission activation	Access control decision	Permission modification and revocation	Policy	Contextual elements	Key generation	Permission assignation	Permission revocation	Access control decision	Encryption and decryption	Management of contextual elements	Data protection and storage
RBAC, 1998		●			●		N/A	●			N/A		
OrBAC, 2003				●	●	●	N/A				N/A		
CP-ABE, 2007			●	○					○	●	●		
FB-CAAC, 2020		●	○	●	●	●	N/A				N/A		
Extended UCON, 2022				●	●	●	N/A				N/A		

Highlights

DCS protects data instead of networks or applications and is supported by NATO

DCS incorporates 4 properties: labelling, formatting, cryptographic protection and context

DCS is implemented using an access control and encryption mechanism

Centralized DCS has limitations for certain cases: **decentralization**, **dynamicity**

There is no access control approach that considers all decentralization and dynamicity criteria

➔ Questions?

References

[1] NATO Standardization Office (NSO), Standardization Agreement 4774 (STANAG-4774) : Confidentiality Metadata Label Syntax, Technical Report NSO/1513(2017)CAP1/4774, North Atlantic Treaty Organization, 20 December 2017.

[2] NATO Standardization Office (NSO), Allied data processing publication 4774 (ADatP4774) : Confidentiality Metadata Label Syntax, Technical Report Edition A Version 1, North Atlantic Treaty Organization, 20 December 2017.

[3] Penders, Ate, Max Van Der Horst, Alex Van Der Linden, Maurits De Graaf, Thomas Quillinan, et Gregor Pavlin. « A Secure Information Management and Interoperability Framework: Enabling Distributed Fusion Engines for Military IoT Applications ». In 2024 International Conference on Military Communication and Information Systems (ICMCIS), 1-10. Koblenz, Germany: IEEE, 2024. https://doi.org/10.1109/ICMCIS61231.2024.10540844.

[4] R. S. Sandhu, Role-based access control, in: Advances in computers, volume 46, 1998, pp. 237–286. doi:10.1016/S0065-2458(08)60206-5.

[5] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, G. Trouessin, Orbac: un modèle de contrôle d'accès basé sur les organisations, Cahiers francophones de la recherche en sécurité de l'information 2 (2003) 30–40.

[6] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Symposium on security and privacy, 2007, pp. 321–334. doi:10.1109/SP.2007.11.

[7] T. Okamoto, K. Takashima, Decentralized attribute-based encryption and signatures, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 103 (2020) 41–73. doi:10.1587/transfun.2019CIP0008.

[8] A. Kayes, R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha, I. Kumara, A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues, Sensors (2020) 2464. doi:10.3390/ s20092464.

[9] G. Abirami, R. Venkataraman, Performance analysis of the dynamic trust model algorithm using the fuzzy inference system for access control, Computers & Electrical Engineering 92 (2021) 107132. doi:10.1016/j.compeleceng.2021.107132.

[10] A. Hariri, A. Ibrahim, T. Dimitrakos, B. Crispo, Wip: Metamodel for continuous authorisation and usage control, in: Proceedings of the 27th ACM Symposium on Access Control Models and Technologies, 2022, pp. 43–48. doi:10.1145/3532105.3535039.

[11] S. F. Aghili, M. Sedaghat, D. Singelée, M. Gupta, MLS-ABAC: Efficient multi-level security attribute-based access control scheme, Future Generation Computer Systems 131 (2022) 75–90. doi:10.1016/j.future.2022.01.003.

[12] S. Xiao, A policy language for context-aware access control in zero-trust network, Master of science thesis, Technological University of the Shannon, 2023.