Cybersecurity Essentials and Management for Energy Sector

CSP001_C_E

PRESENTATION BY:
CRISTINA ALCARAZ
UNIVERSITY OF MALAGA, SPAIN

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Topic-6: Security Controls Selection and Implementation for Energy Environments

Overview

- Select and implement appropriate security controls based on the specific needs of energy systems
- Implement strong password policies and multi-factor authentication (MFA) to protect user accounts
- Encrypt sensitive data at rest and in transit to prevent unauthorised access and data breaches
- Regularly apply security updates and patches to software systems to address vulnerabilities

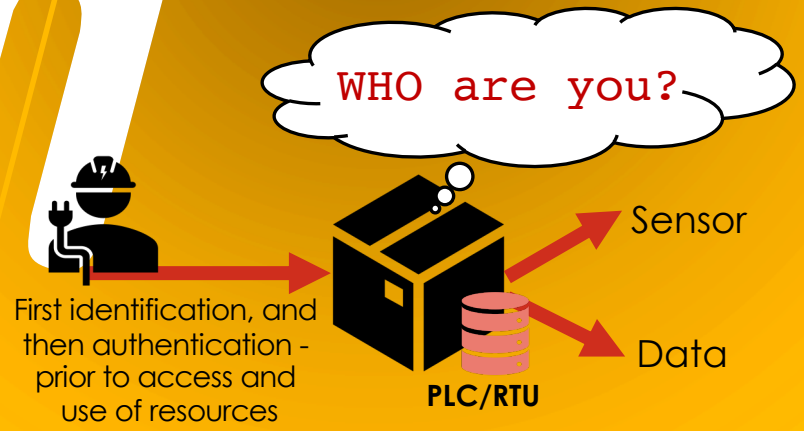
Topic-6: Security Controls Selection and Implementation for Energy Environments

Overview

- Select and implement appropriate security controls based on the specific needs of energy systems
- **Implement strong password policies and multi-factor authentication (MFA) to protect user accounts**
- Encrypt sensitive data at rest and in transit to prevent unauthorised access and data breaches
- Regularly apply security updates and patches to software systems to address vulnerabilities

Authentication and identification

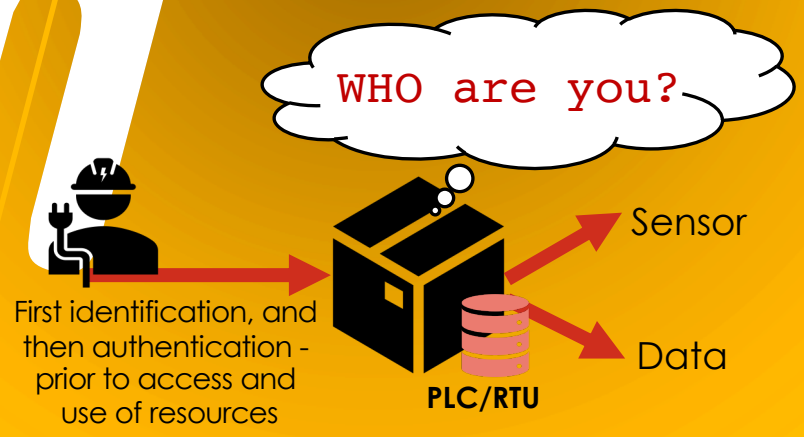
- As discussed previously, the National Institute of Standards and Technology (NIST) defined **authentication** as the way to
  - "*Verify the identity of a user, process or device, often as a prerequisite for allowing access to a system's resources*"
  - This also means that authentication process also includes an implicit **identification** process to identify users, process or devices



Source: CSRC, "Glossary", NIST, 2024.
URL: https://csrc.nist.gov/glossary

Authentication and identification

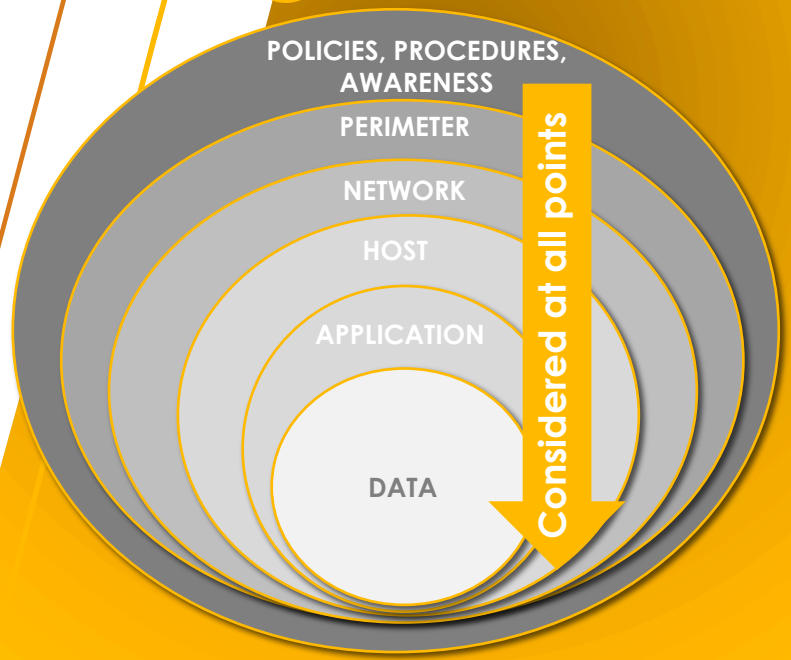
- As discussed previously, the National Institute of Standards and Technology (NIST) defined **authentication** as the way to
  - "*Verify the identity of a user, process or device, often as a prerequisite for allowing access to a system's resources*"
  - This also means that authentication process also includes an implicit **identification** process to identify users, process or devices
- In power systems, these resources can be:
  - The network perimeter and its resources (routers, switches, proxies…)
  - The SCADA server
  - PLC/RTU devices
  - Sensors, actuators
  - Operating Systems
  - Files, databases and repositories
  - Software applications
  - Etc. – *any system or device to which users can have access to*



Source: CSRC, "Glossary", NIST, 2024.
URL: https://csrc.nist.gov/glossary

Authentication in power systems

- In fact, authentication is a paramount requirement in IT/OT-based infrastructures, and corresponds to **the first line of defence**
- This feature is also considered by the European Union Agency for Cybersecurity (ENISA) for Smart Grids
  - In its report on "*Appropriate security measures for smart grids*", it adds the authentication as part of:
    - Logical access control (SM 9.3): "*The provider should enforce logical access to authorised entities on smart grid information systems and security perimeters*"
    - Secure remote access (SM 9.4): "*The provider should establish and maintain secure remote access where applicable to smart grid information systems*"
  - For both conditions, it is essential to manage authentication methods and identification measures
- Therefore, authentication MUST also be part of the **defence in depth**, and must be contemplated from a regulatory and technical point of view

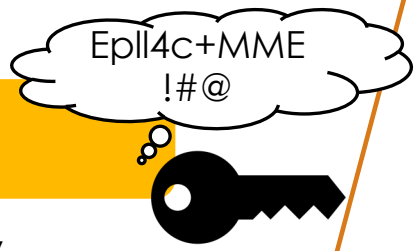


Source: ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

Authentication in power systems

- There are three ways to authenticate:

What do I know?



- Authentication based on information known only by the corresponding entity

What do I have?

- Authentication based on something that the entity possesses

Who am I ?

- Authentication based on a biometric feature

Authentication in power systems

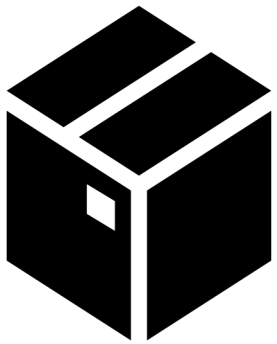
- There are three ways to authenticate:

What do I know?

What do I have?

Who am I ?

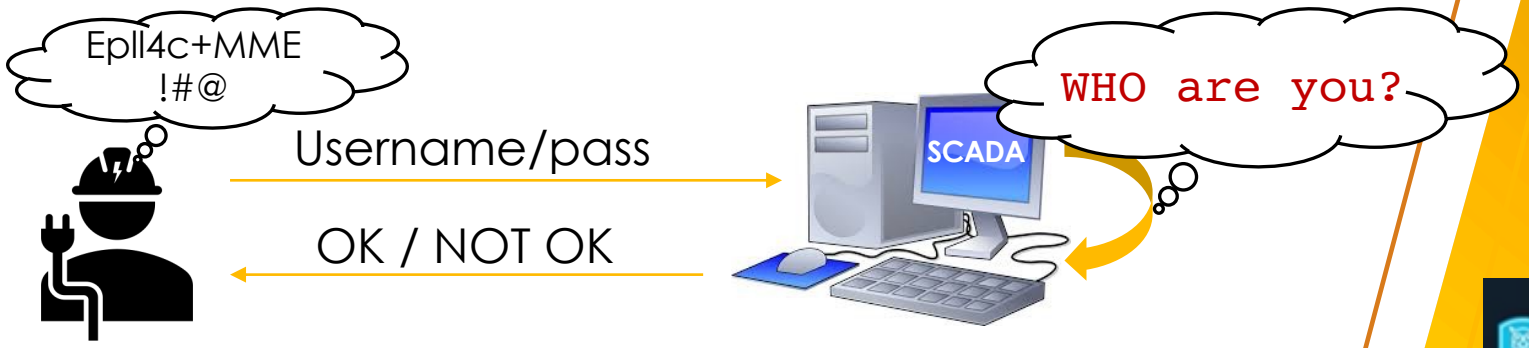
U S E R N A M E /
P A S S W O R D



PLC/RTU
SCADA server
HMIs

Authentication based on username/password

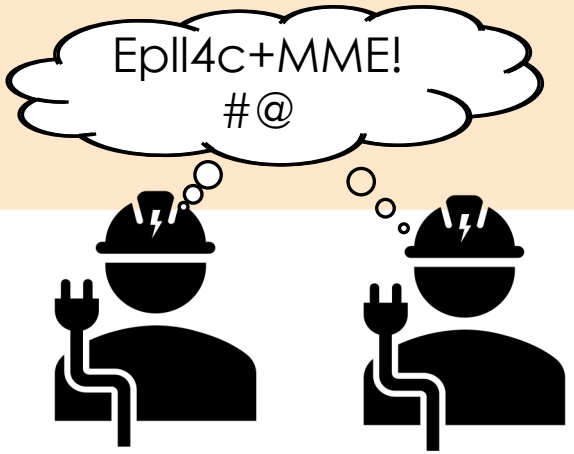
- In **password-based systems**, users, devices and processes MUST be registered with a unique identifier together with a secret to allow access
- The procedure is simple:
  1. The entity first provides at the destination node or authentication server the information necessary for its verification
  2. The destination node or authentication server verifies the identity and the associated secret
  3. If all this information is valid, access is granted



Authentication based on username/password

- In password-based authentication systems, it is assumed that users know certain information that no one else should know: "passwords"
- Nonetheless:

Features	Inconveniences (depending on the token)	Recommendations for policies
• The password can be passed from one user to another user – e.g., in emergency situations • More than one user can use it at a time – e.g., in emergency situations	• It is strictly necessary to use strong passwords, and not to repeat them • Difficult to remember all passwords used • For both reasons, a password manager is often used	• Use long sentences as passwords or complex words with alphanumeric values • Promote regular rekeyings • Avoid rekeyings with simple and related passwords • Set locks by number of attempts • Use robust authentication database servers – with SALT



Authentication based on username/password supported by hash

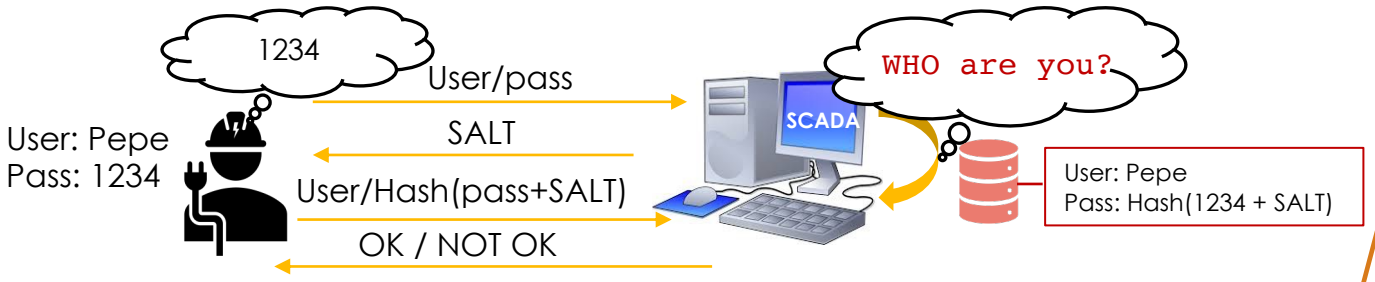
- Passwords should NOT be stored in the clear
  - User accounts stored on a system are normally protected with a "hash" value associated with the password

User: Pepe
Pass: 1234

  - When human operators/users want to log in to a resource, the password is requested, hashed and compared with the stored hashed password

Authentication based on username/password supported by SALT

- However, attackers may be able to launch dictionary attacks / Rainbow Table attacks
  - It consists of preparing a file with all possible HASH combinations to obtain the initial password
- To avoid dictionary attacks, a "**SALT**" value should be used
  - **HASH (PASS + SALT)** such that SALT is a large random number (minimum 10 values)



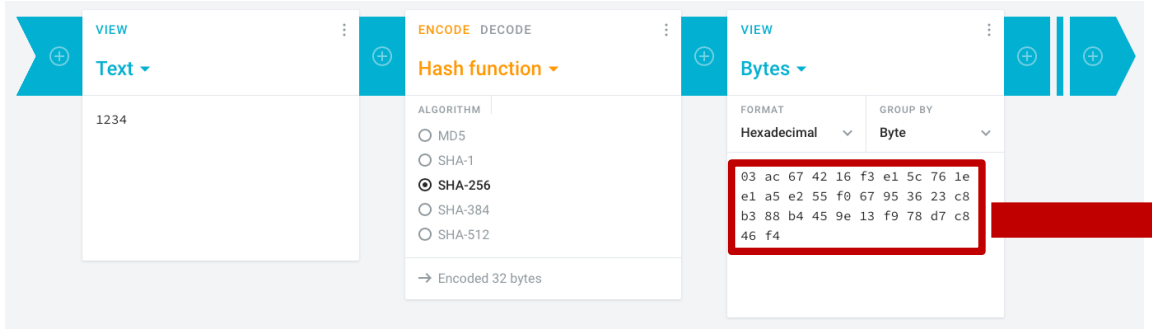
  - It is also recommended:
    - Not to reuse the same salt values in the following rekeyings
    - Use robust (and slow) hash functions, such as PBKDF2*, bcrypt, or Argon2id

Dictionary attack

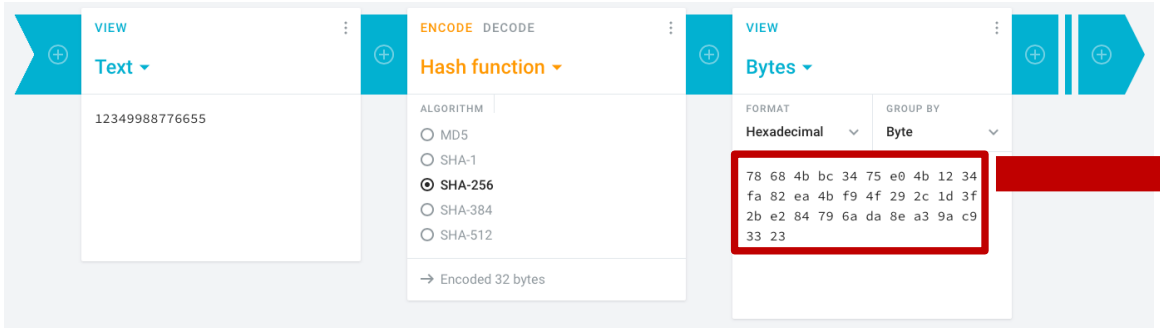
H(1234) → failed
H(1234Mom) → failed
H(1234Mylove) → failed
H(1234Daughter) → success !

Authentication based on username/password with SALT support

- A quick way to put this lesson into practice is to use the online tool **cryptii** (https://cryptii.com):
  - Create a hashed password (1234)



  - Create a hashed password + SALT (9988776655)



The two outputs (or hashes) are completely different for different input values - one being more robust than the other

AUTHENTICATION IN POWER SYSTEMS

Source: Wierk, Cryptii, 2024.
URL: https://cryptii.com

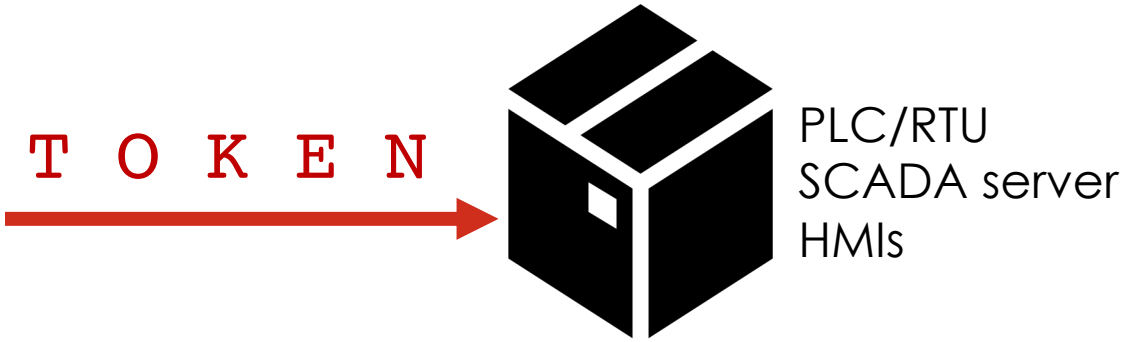
Authentication in power systems

- There are three ways to carry out the authentication process:

What do I know?

What do I have?

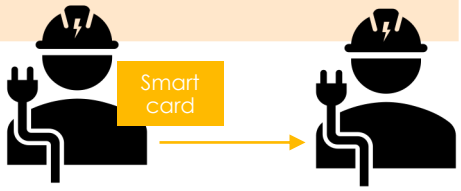
Who am I ?



Authentication based on token

- In **token-based authentication systems**, operators/users possess a physical object that in some way proves their identity such as:
  - Smartcards, USB key, digital certificates (containing the public key of the human operators), etc.
- Nonetheless:

Features	Inconveniences (depending on the token)
• The token can be passed from one user to another – except certificates • Only one user can use it at a time	• They do not actually prove the identity of the users • Anyone in possession of the token gets to be authenticated • In case of loss or damage, the legitimate user is left without the possibility to be authenticated • The token may sometimes be forged



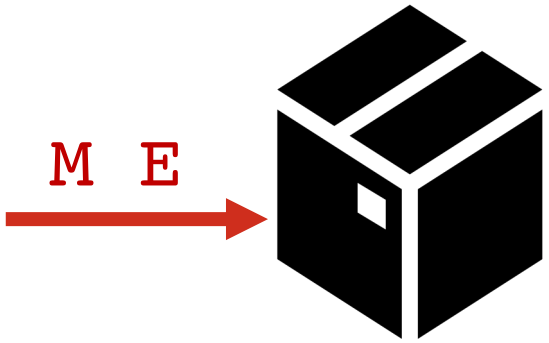
Authentication in power systems

- There are three ways to carry out the authentication process:

What do I know?

What do I have?

Who am I ?



PLC/RTU
SCADA server
HMIs

Authentication based on biometric

- In **biometric-based authentication systems**, certain information is extracted from the user's biological characteristics (fingerprint, iris, voice, etc.)
- Nonetheless:

Features	Inconveniences
• Biometric data cannot be transferred from one user to another • Only the user can use his/her biometric factors	• The user profile must be stored on the computer before authentication can take place • These systems require special protection measures • Storage of biometric data in secure elements to prevent leakage of sensitive data • These systems are more expensive than the previous systems • If a biometric factor is lost, it is lost forever - for example, a fingerprint due to a burn • Not all biometric factors are suitable for industrial ecosystems, such as voice - due to industrial noise

User authentication - 2FA, others

- So far, we have seen the most typical authentication factors, but these can be combined with others
- For example:
  - With something that indicates my POSITION
    - **Location-based authentication** at the time of doing the operation
    - **IP-based authentication** – similar purpose
  - With something that I DO
    - **User behaviour-based authentication**, such as pressing a key, operating a screen, etc.
  - With something that indicates the CONTEXTUAL STATE
    - **Context-based authentication**, such as high industrial noise, high temperature of the area, high radiation or intoxication for operators, etc.

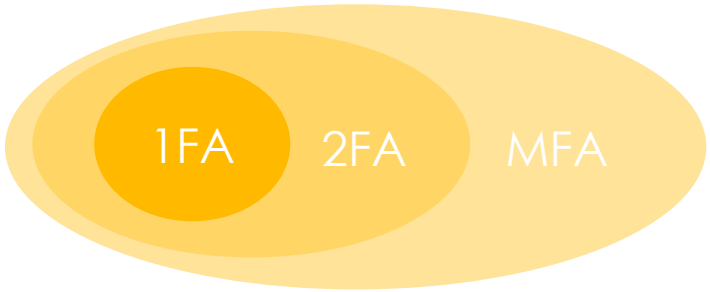
User authentication - 2FA, others

- So far, we have seen the most typical authentication factors, but these can be combined with others
- For example:
  - With something that indicates my POSITION
  - With something that I DO
  - With something that indicates the CONTEXTUAL STATE

- The combination of authentication factors results in **multi-factor authentication**
  - 1FA (single-factor): When 1 of the above mechanisms is applied
  - 2FA (two-factor): When 2 of the above mechanisms are combined (e.g., password + token)
  - MFA (multi-factor): More than 2 combinations apply (e.g. pass + token + biometrics)

User authentication - 2FA, others

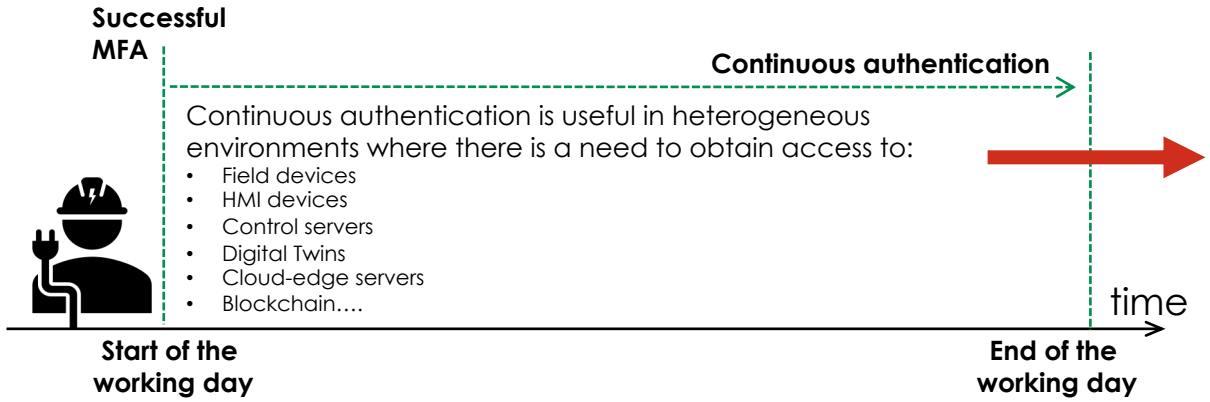
- The higher the combination, the more robust the verification process will be, resulting in **strong authentication**
  - This avoids, for example, potential impersonation risks by creating authentication layers that verify the identity of an entity several times



- We could adapt the 2MFA conventional applications in energy control systems, such as:
  - Google Authenticator or Microsoft Authenticator
    - Both deal with random codes to allow secure access to online services, such as user accounts
    - I.e., provides a double check, at least on user accounts considered as "high risk"

User authentication - 2FA, others

- The use of MFA is also supported by existing directives such as the European **NIS2 (Network and Information Security)** - DIRECTIVE (UE) 2022/2555
  - Covering critical sectors such as "energy", including electricity, heating and cooling, oil, gas and hydrogen
  - The directive remarks the significance of the use of **multi-factor authentication and continuous authentication** solutions



Relevant **benefits of continuous authentication** arise:

- More productivity by reducing the authentication process in each access
- Transparency for IT/OT administrators, engineers, managers... - although this depends on the approach
- High security guarantees

Source: Directive (EU) 2022/2555 of the European Parliament and of the Council, 2022
URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27

Final remarks

- Throughout this topic, we have seen the most relevant authentication factors in the literature
  - Exploring their significance and capacity for their combination
- Particularly, we have explored:
  - 1FA, based on what I know, I have, I am, I do, …
  - 2FA , based on the combination of two factors
  - MFA, based on the combination of more factors
- But we have also seen the need to consider regulatory frameworks that support the technique
  - Especially those focusing on the energy sector such as NIS2 Directive
- In NIS2, the concept of 'continuous authentication' is mentioned
  - The approach may add significant value to the production chain, and may support the emergence of situations if authentication techniques are applied correctly
  - However, not all approaches are effective: the use of biometric factors may be appropriate, but in certain industrial environments it may be difficult to apply

References and sources

1. CSRC, "Glossary", NIST, 2024.
   URL: https://csrc.nist.gov/glossary
2. Wierk, Cryptii, 2024.
   URL: https://cryptii.com
3. ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012.
   URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids
4. Directive (EU) 2022/2555 of the European Parliament and of the Council, 2022.
   URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27
5. DeepL Translator for Proofreading:
   https://www.deepl.com/translator

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

If you have any questions, please do not hesitate to contact:

- Cristina Alcaraz
  Associate Professor
  University of Malaga
  alcaraz@uma.es