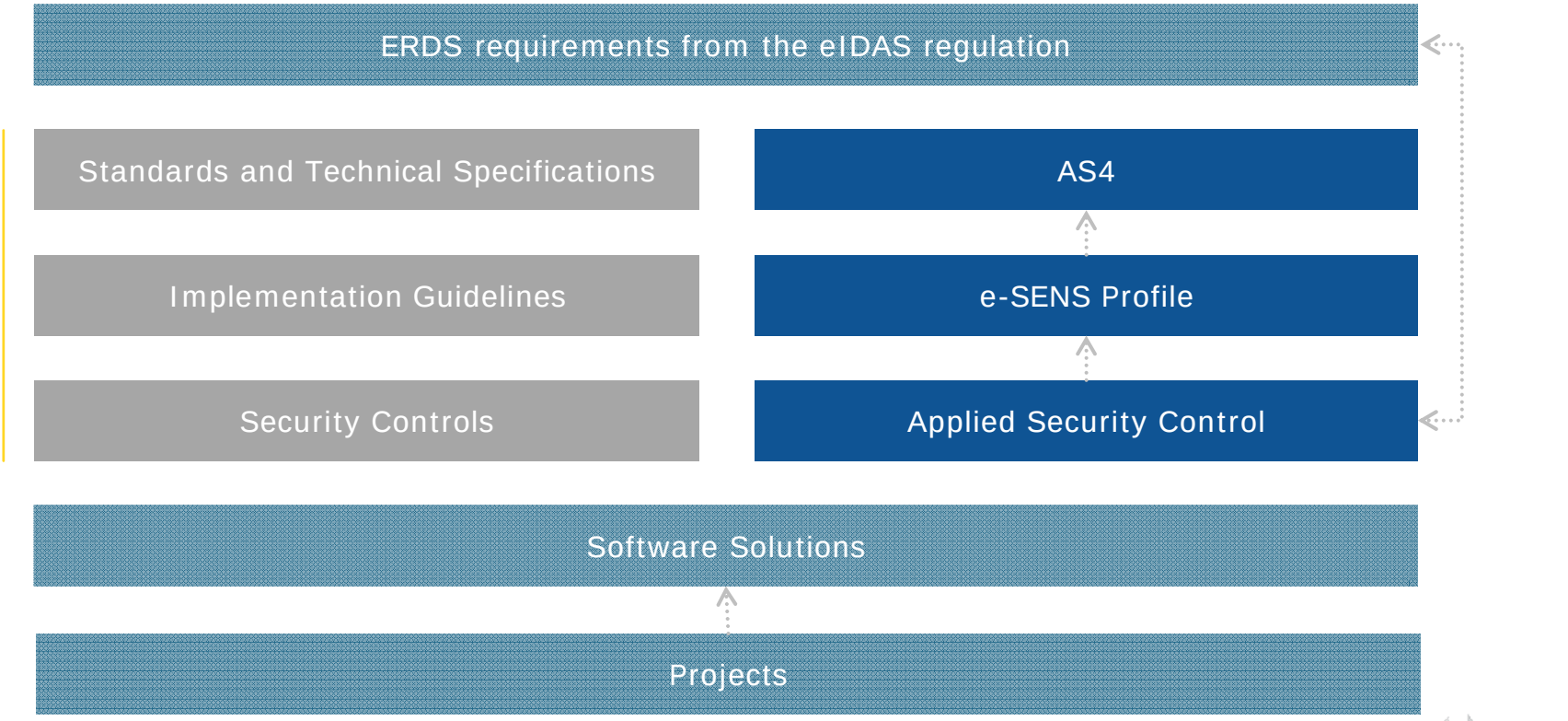
CEF eDelivery Security Controls – Graphics

Graphics based on the Four-corner model

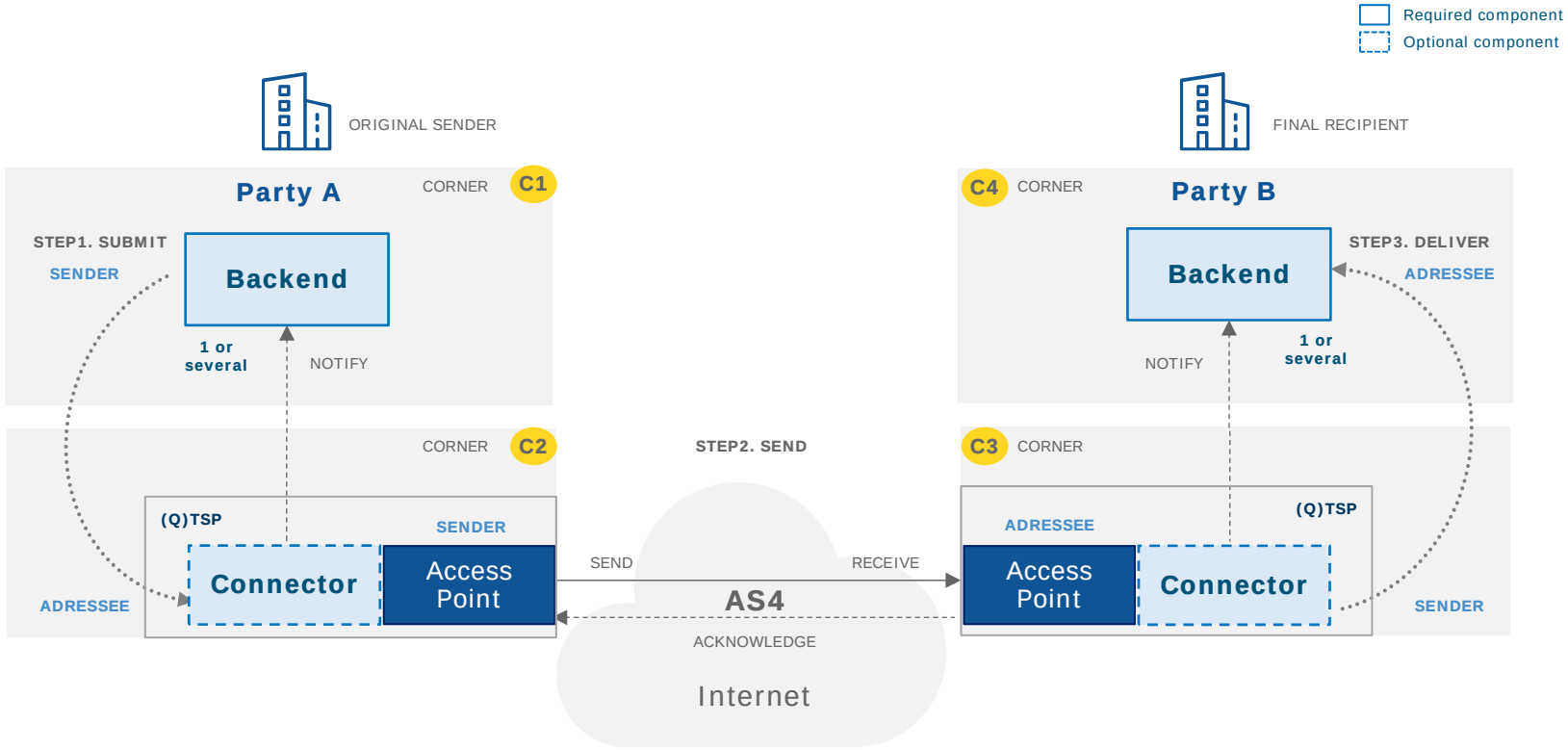
Gábor Bartha

DG CONNECT – unit H4-eGovernment and Trust

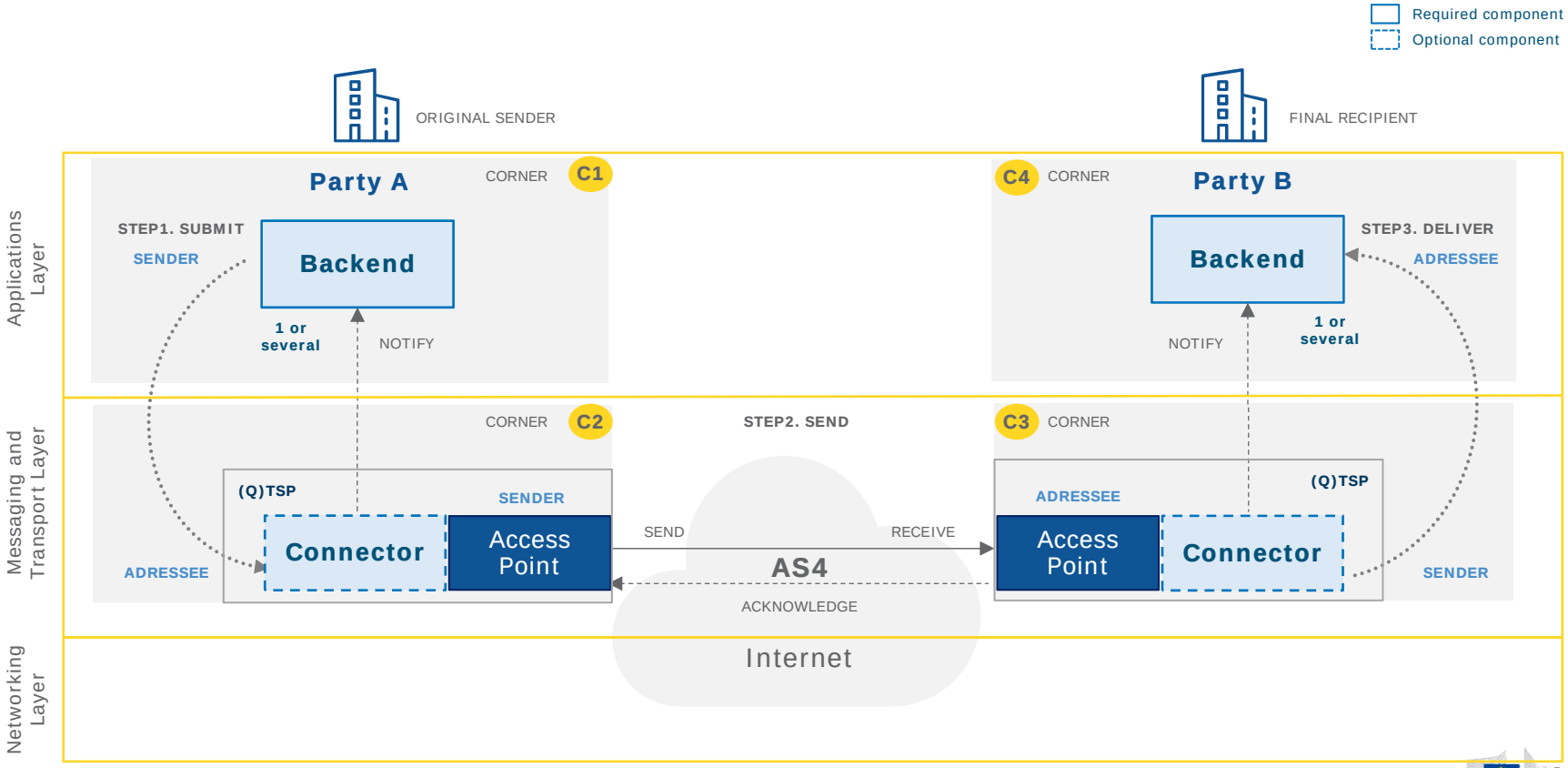
Approach to link eDelivery and eIDAS ERDS



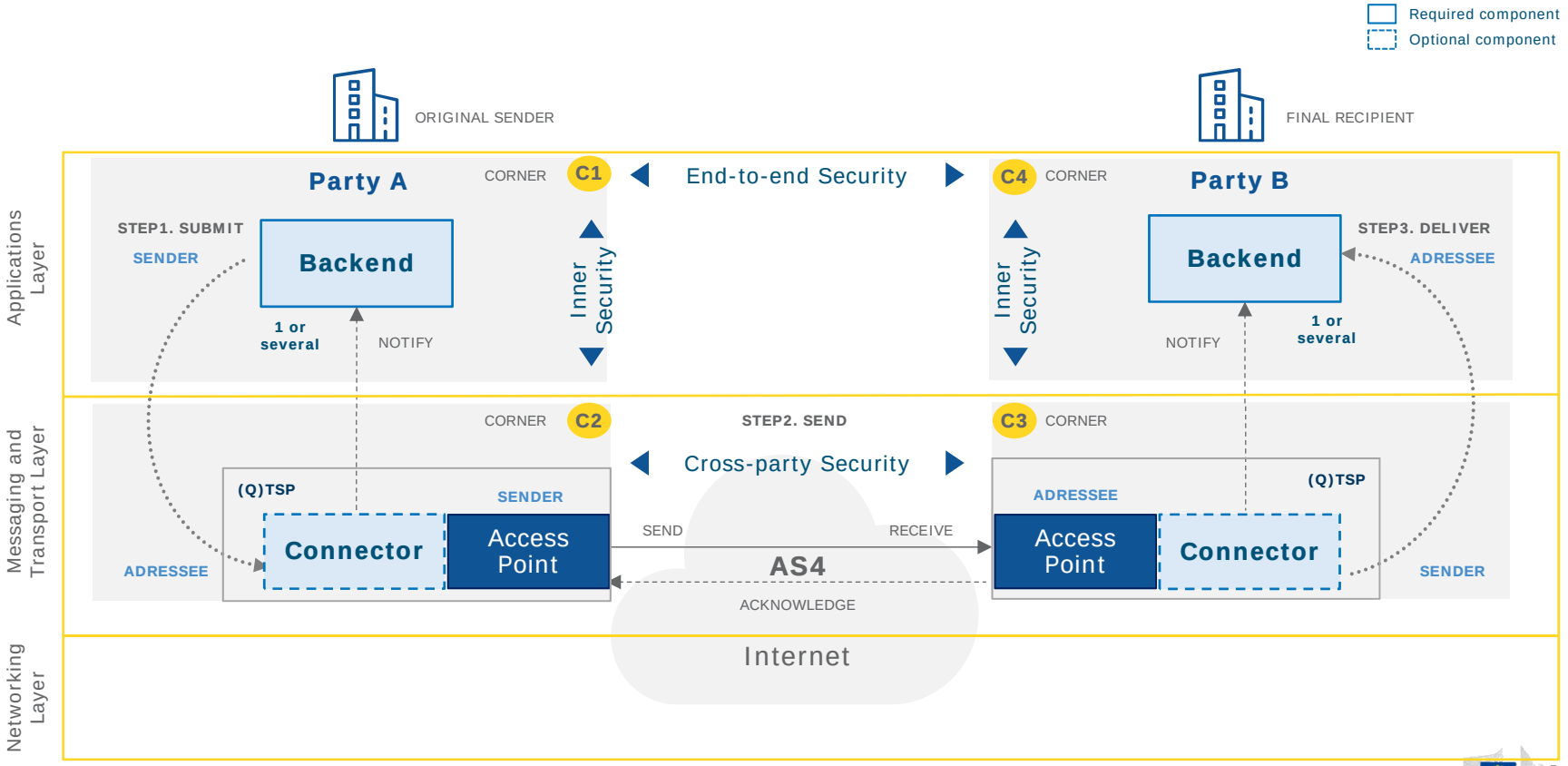
eDelivery Messaging Infrastructure based on the 4-Corner Model



eDelivery Messaging Infrastructure based on the 4-Corner Model



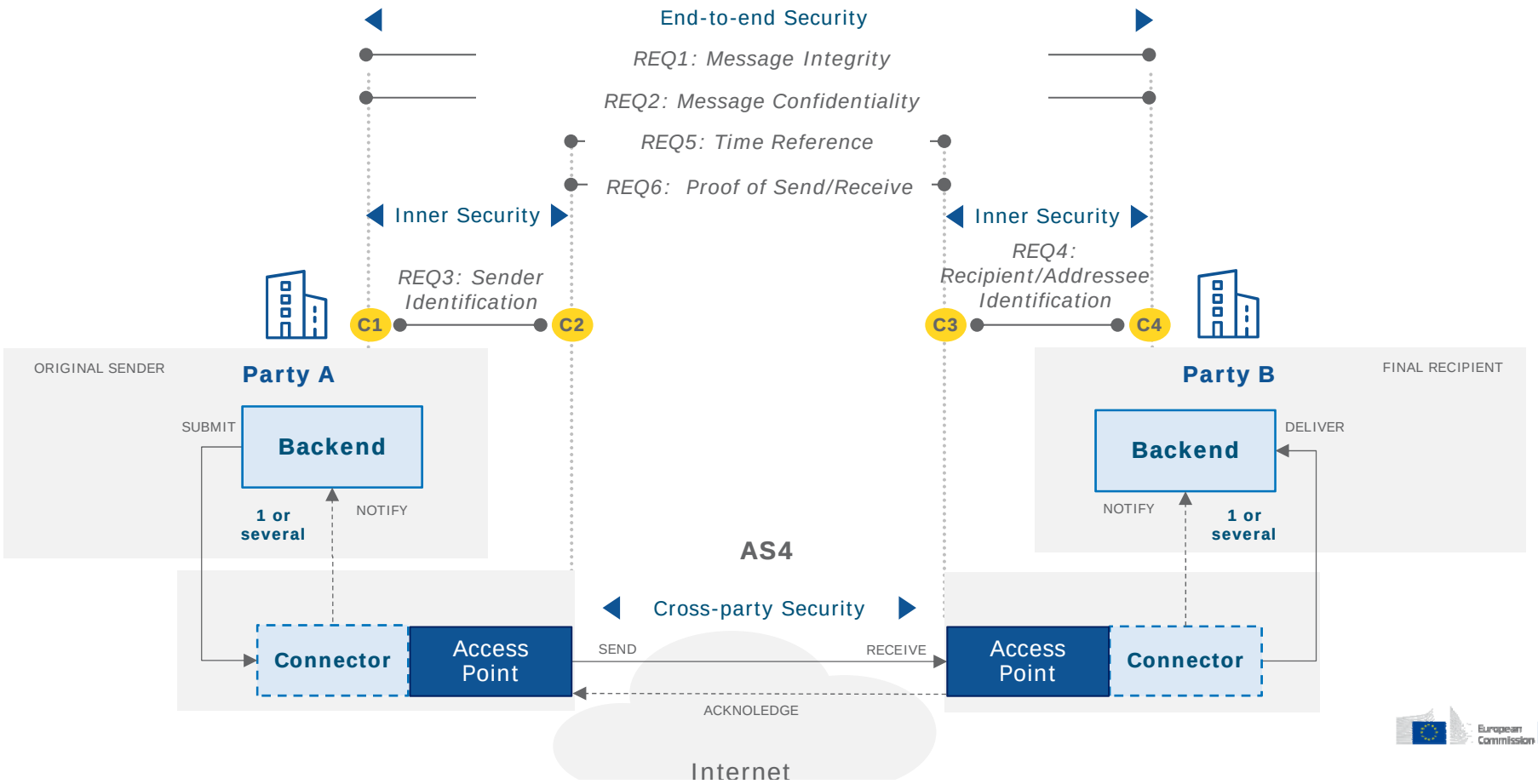
eDelivery Messaging Infrastructure based on the 4-Corner Model



Summary of ERDS requirements from the eIDAS regulation

Requirement	Description	eIDAS reference
REQ1 **Message Integrity**	Messages should be secured against any modification during transmission.	Article 3 (36) Article 19 Article 24 Article 44, (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
REQ2 **Message Confidentiality**	Messages should be encrypted during transmission	Article 5 Article 19 Article 24
REQ3 **Sender Identification**	The identity of the sender should be verified.	Article 24 Article 44 (b) they ensure with a high level of confidence the identification of the sender;
REQ4 **Recipient / Addressee Identification**	Recipient / addressee Identity should be verified before the delivery of the message.	Article 24 Article 44 (c) they ensure the identification of the addressee before the delivery of the data;
REQ5 **Time-Reference**	The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp.	Article 44 (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
REQ6 **Proof of Send/Receive**	Sender and receiver of the message should be provided with evidence of message recipient and deliver.	Article 3 (36) "… provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data…"

Mapping of ERDS Requirements to the 4-Corner Model



Summary of security controls

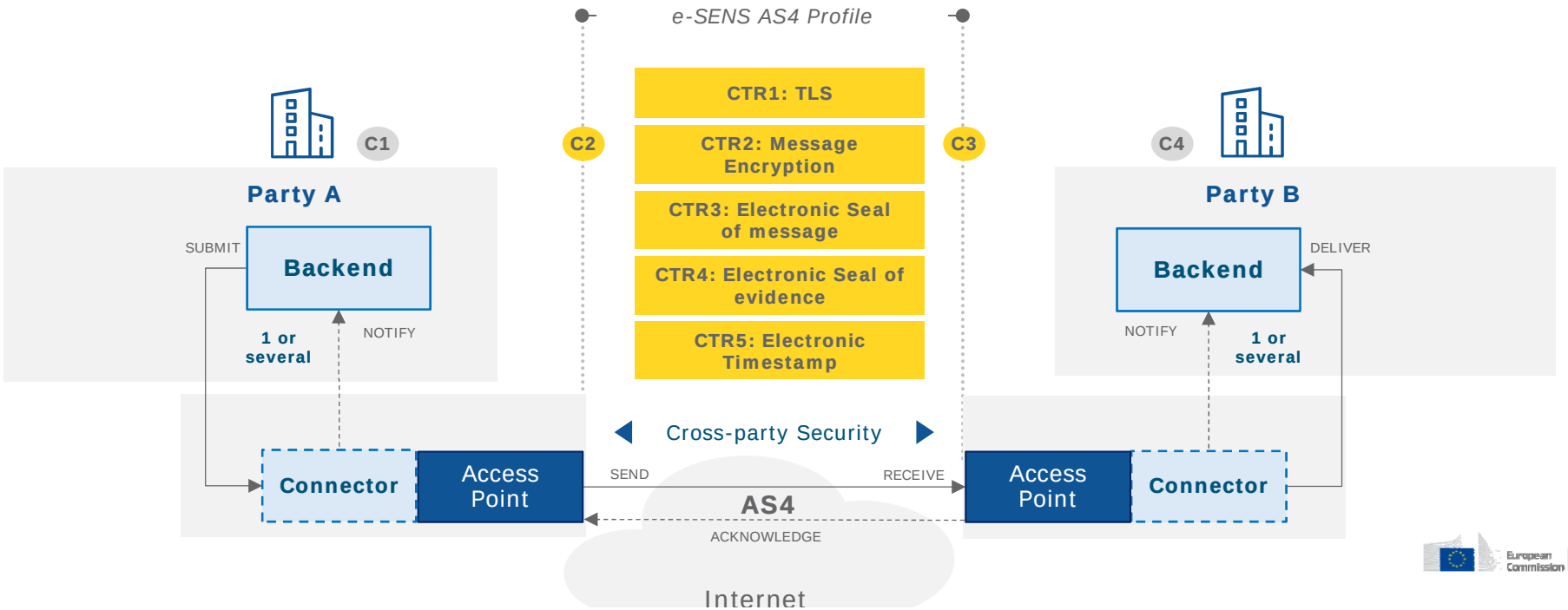
(*) Not exhaustive and it is by no means a guarantee that the system will be granted qualified status under the eIDAS regulation. For the process of granting the qualified status, please refer to the national supervisory body in the respective country.

Security control	Legal implications
CTR1 **Transport Layer Security (TLS) + Authentication** TLS protocols ensure authenticity and integrity of the message, by applying host to host cryptographic mechanisms	European General Data Protection Regulation (GDPR), in case of applicability.
CTR2 **Message Encryption** Message encryption ensures confidentiality of the message payload so that only the correct recipient can access it	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: **Electronic Seal of message** From technical perspective, electronic seal ensures integrity of the message header and payload and authenticity of origin	**Non-qualified**: Ensures integrity and origin of the data, in other words its authentication **Qualified**: eIDAS Regulation, Article 35. “A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data” **Both**: Non-discrimination in legal proceedings
CTR4: **Electronic Seal of evidence** Provides evidence to the sender C1 that the message was sent, delivered to the final recipient C4 and authenticity of destination	
CTR5: **Electronic Timestamp** Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time	**Non-qualified:** Ensures date and time of the data. **Qualified:** eIDAS Regulation, Article 41. “A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.” **Both:** Non-discrimination in legal proceedings

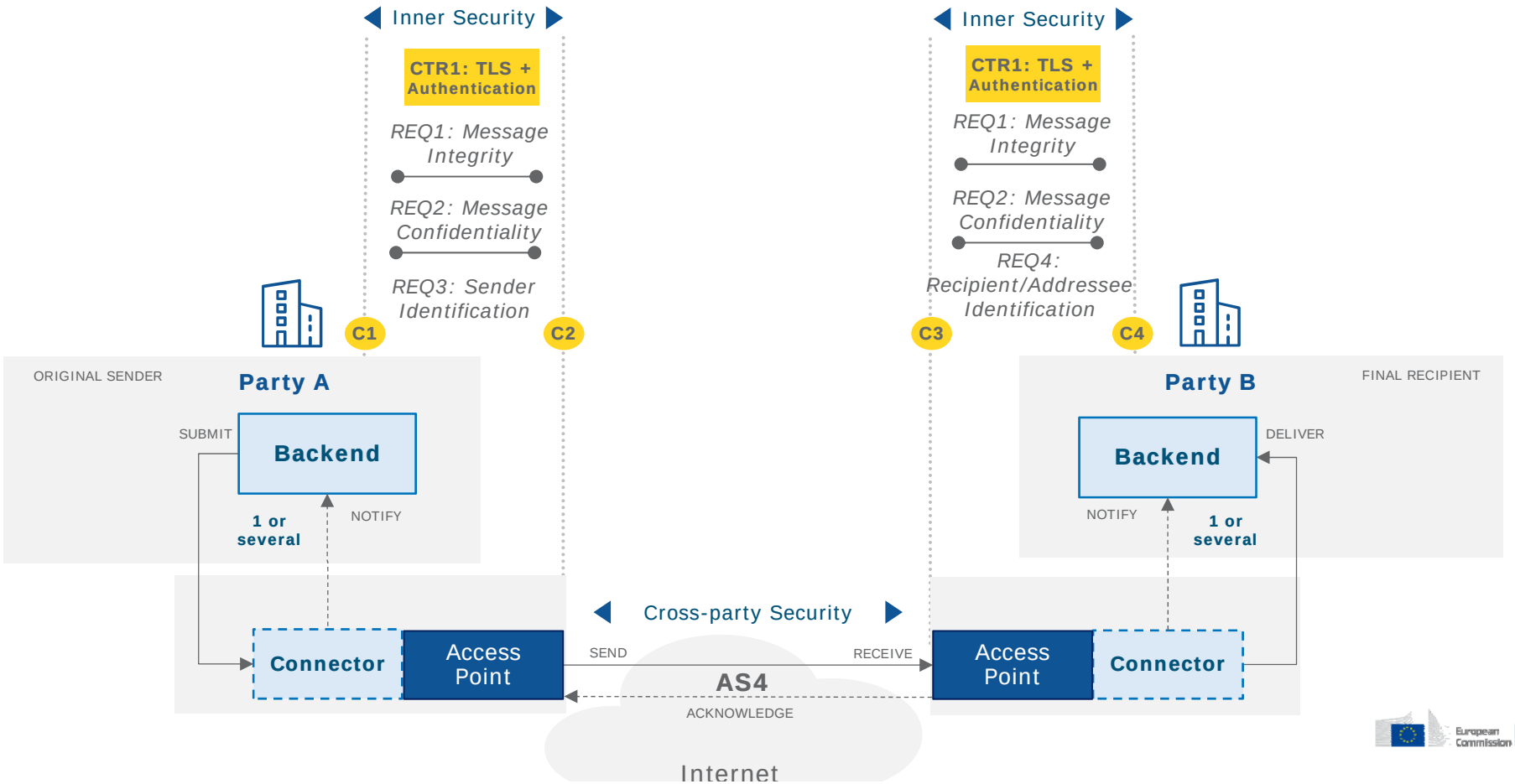
List of security controls applied to the e-SENS AS4 message protocol

Security control	Description
CTR1 **Transport Layer Security (TLS)**	Transport Layer Security (TLS 1.2 [9]) protocol is used, following ENISA security [7] and BSI [8] guidelines. For the sender identification is provided as follows: • Basic authentication: C2 uses username/password to authenticate to C3. In this case, proper password management, including secure storage, sufficient complexity and regular updates need to be ensured by C2; • Mutual authentication: This is done using the digital certificate of C2, allowing C3 to identify C3.
CTR2 **Message Encryption**	C2 encrypts the payload of the message using AES-GCM with a random secret key, and the random key with the public key of C3 using RSA-OAEP. Message encryption follows WS-Security using W3C XML Encryption The used cipher suite for symmetric encryption is: AES GCM-mode, and for asymmetric: RSA-OAEP. This should follow the ENISA security [7] and BSI [8] guidelines.
CTR3: **Electronic Seal of message**	C2 applies an electronic seal to the message header and payload using its own private key which guarantees integrity protection. The seal is verified by C3 using C2 public key for authenticity and non-repudiation of the message payload and headers. Electronic sealing follows WS-Security with W3C XML Signing. The cipher suite is RSA-SHA256.
CTR4: **Electronic Seal of evidence**	Electronic seal is applied to the receipt. Upon reception and verification of a message from C2, C3 generates an evidence receipt based on message identification information (e.g., message identifier, timestamp, and sender metadata) with a new timestamp and a reference to the received message, applies an electronic seal and returns the sealed evidence to C2. The receipt is sent automatically to C2 as a “signal” message response to the initial message. Electronic sealing follows WS-Security with W3C XML Signing. The used cipher suite is: RSA-SHA256.
CTR5: **Electronic Timestamp**	Timestamp is placed at the WS-Security header, and it is electronically sealed for integrity protection. At this moment, by default, it is not a qualified time stamp and it relies on the system clock.

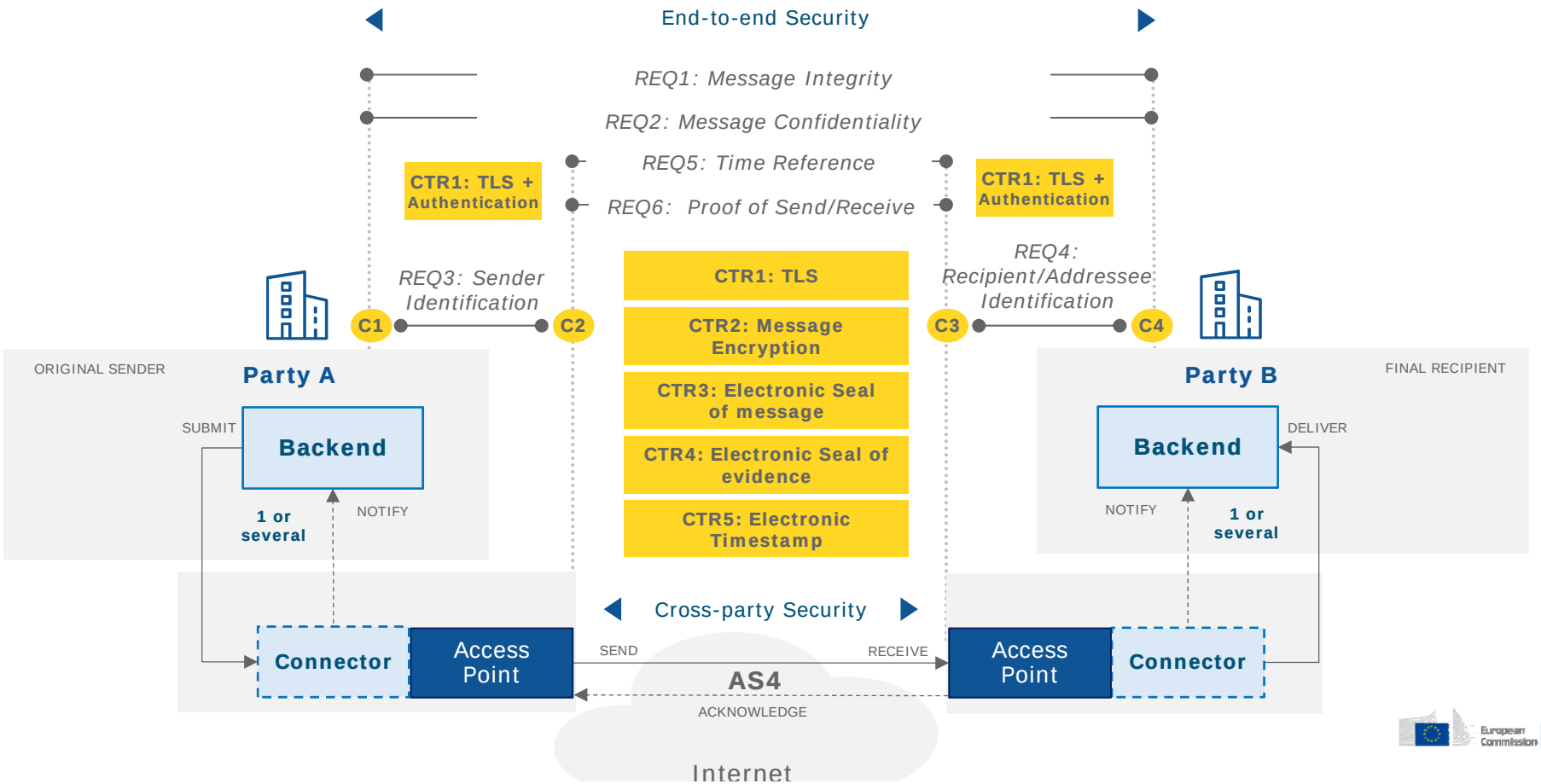
Mapping of ERDS Requirements to the 4-Corner Model



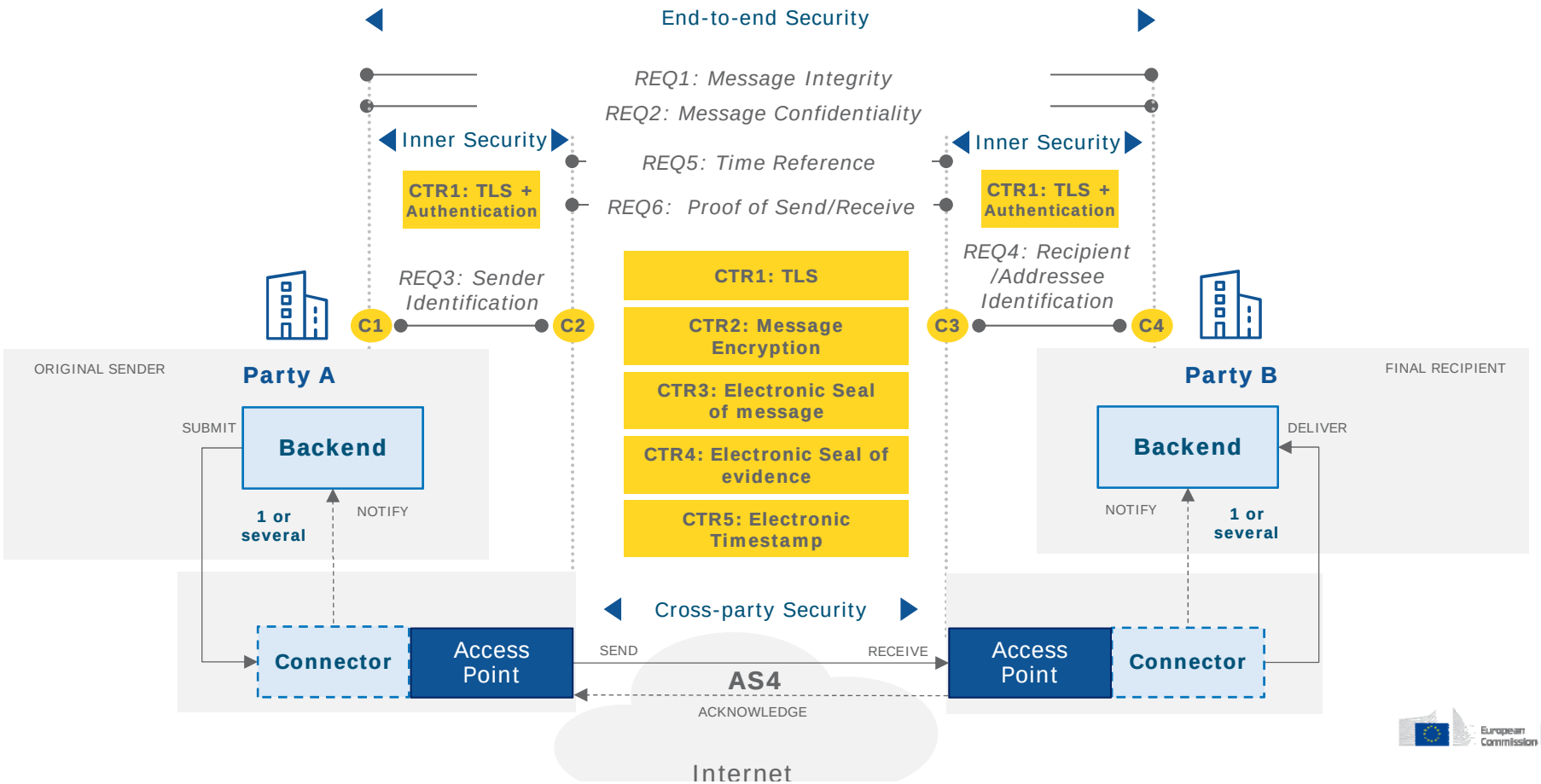
Mapping of ERDS Requirements to the 4-Corner Model



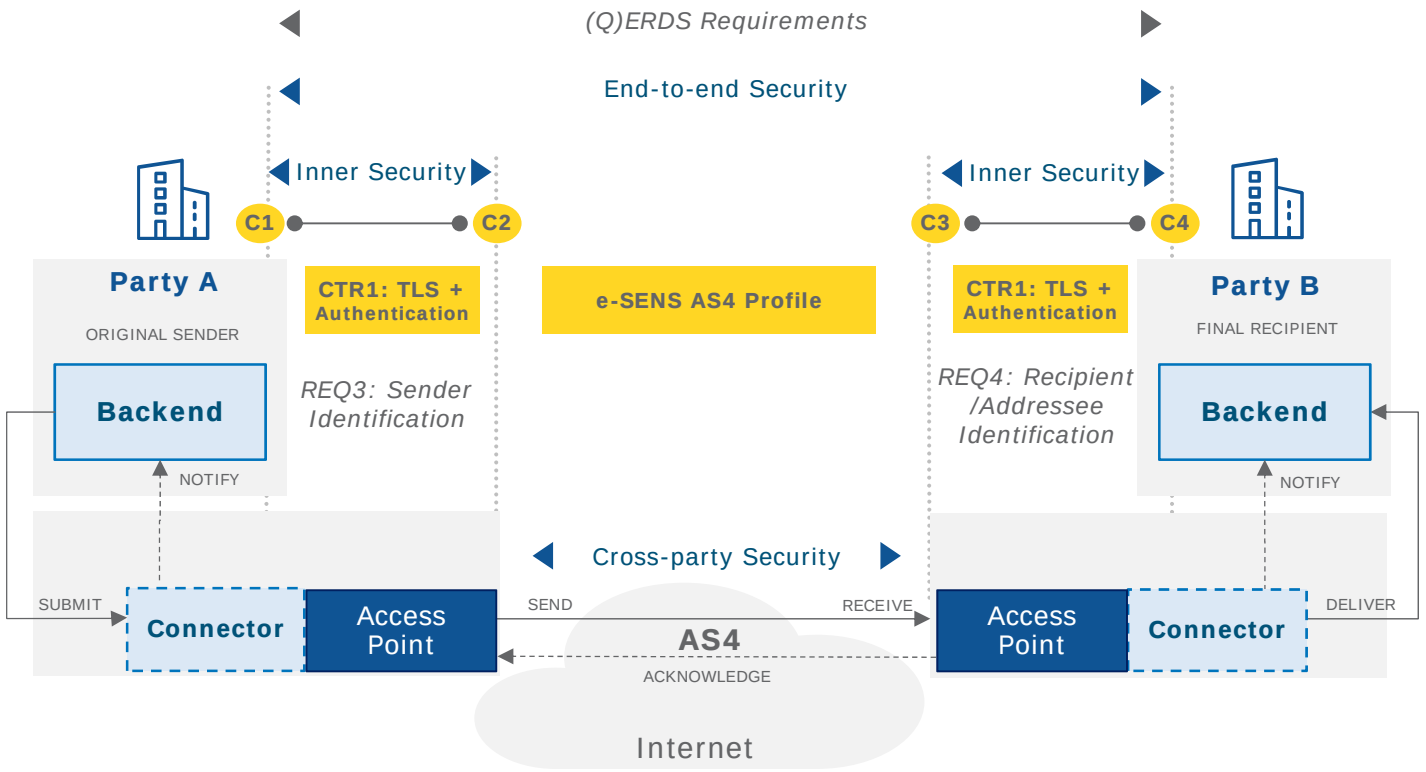
Mapping of ERDS Requirements to the 4-Corner Model



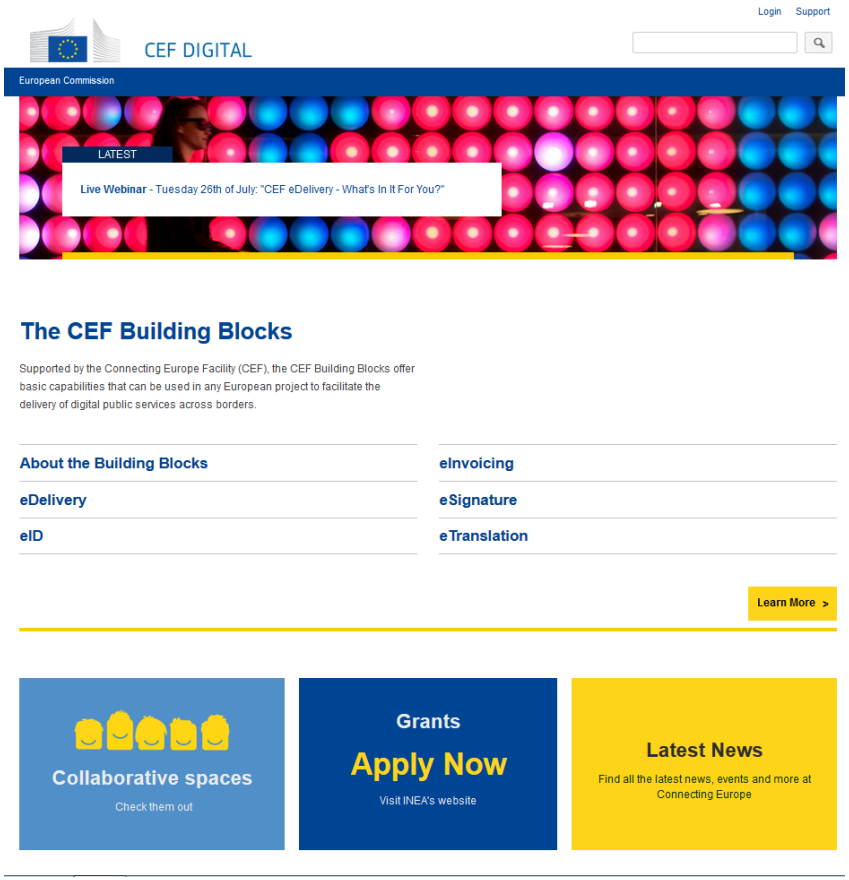
Mapping of ERDS Requirements to the 4-Corner Model



Mapping of ERDS Requirements to the 4-Corner Model



Find out more on CEF Digital



DIGIT
Directorate-General for Informatics

DG CONNECT
Directorate-General for Communications Networks, Content and Technology

Contact us

CEF-BUILDING-BLOCKS@ec.europa.eu