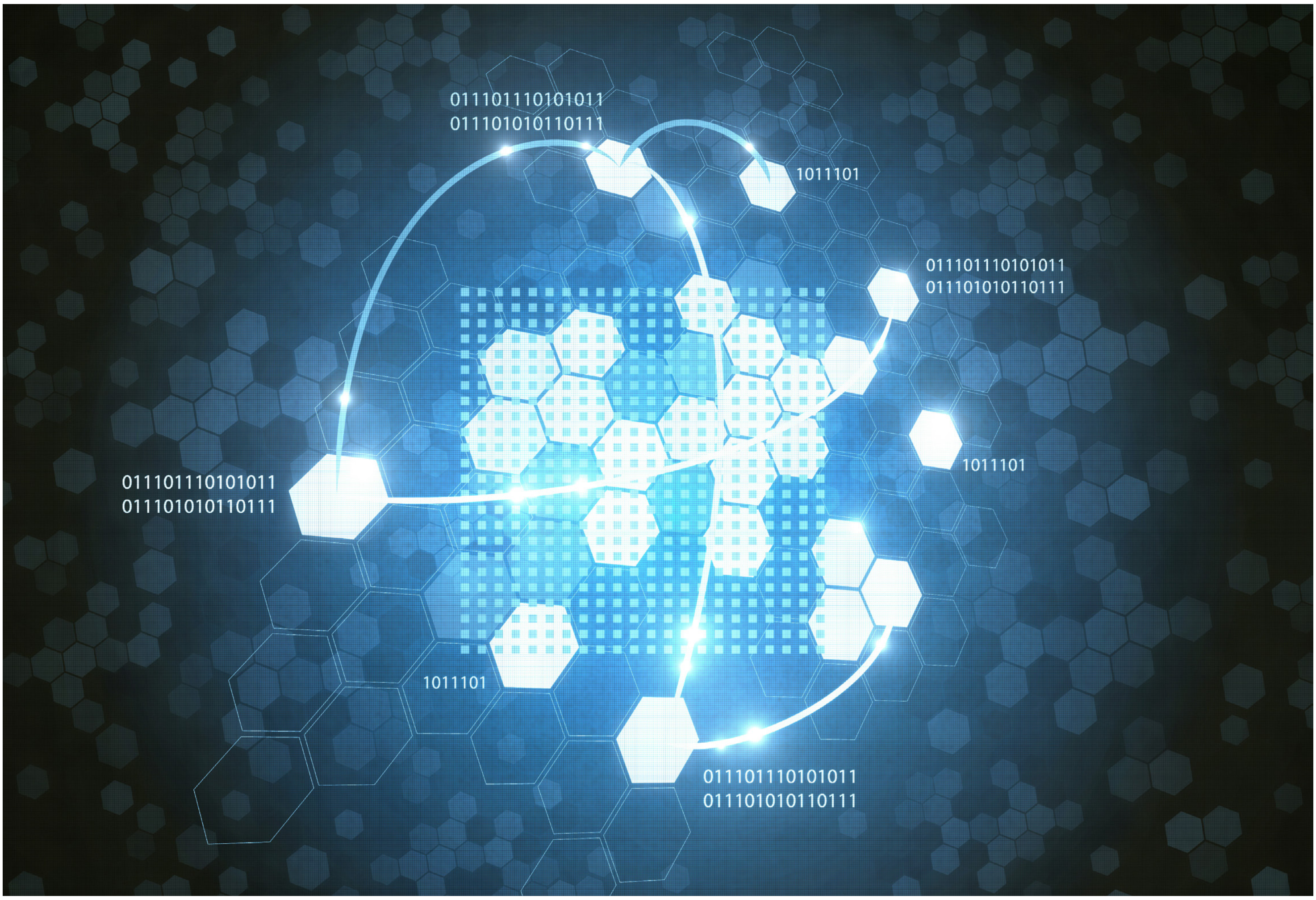
Baltus 2.0
White paper



This White Paper explains what we aim to achieve by developing the BALTUS 2.0 infrastructure.

The existing infrastructure for on-line payment and information exchange (BALTUS and BDM) are a result of more than 40 years of cooperation and self governance within the Norwegian finance sector.

The needs

Analysis has revealed risks and areas for potential improvement of the infrastructure. The following top bullet points establish the foundation for why we have started improving the infrastructure:

- **Timely Open Source** – The industry wants to eliminate dependencies to legacy software and secure availability of qualified knowhow.
- **Support End-to-End Security** – There is a need for even more flexibility and efficiency regards to methods for securing transactions in multi system environment.
- **Facilitate collaboration** – The industry wants to lower the threshold for entering into the market for Information and communications technology (ICT) vendors (i.e. increased competition) and ease innovation.
- **Availability** – There is a need to reduce vulnerabilities from incidents and errors in the network and induce fast recovery when severe incidents have occurred.
- **Strengthen governance** – There is an increasing level of enforcement from International and national regulation authorities regarding governance, addressed to this type of collaborative infrastructures.

What is BALTUS 2.0?

BALTUS 2.0 is a set of documents describing the requirements for the BALTUS 2.0 infrastructure and interaction with surrounding IT-environments.

BALTUS 2.0 is not a software solution. Hence the dependency to legacy software is eliminated, and the requirements constitutes the “documentation package” which shall be maintained in order to conserve know-how and support the new and rapidly changing demands in the financial industry.

Hence the trend in development for even more secure transportation of transactions, the end-to-end security features must be handled in the business applications, outside the BALTUS 2.0 infrastructure. Therefore the BALTUS 2.0 functionalities are designed to handle distribution and addressing only, regardless of the transaction content or securing functionality.

The BALTUS 2.0 requirements regulate Governance, Network and Security, Technical specifications for nodes and the central routing table.

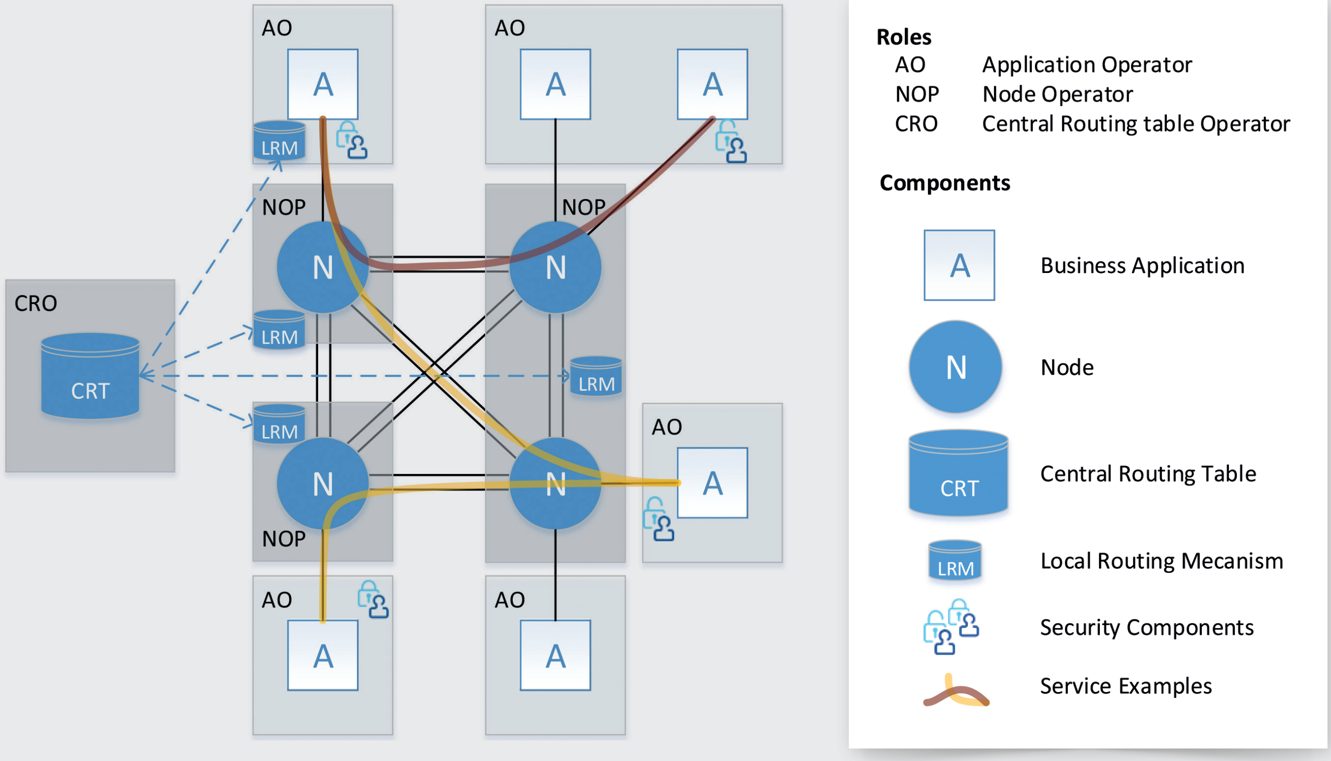
The model below describes the different roles, dependencies and transaction flow in BALTUS 2.0.

When BALTUS 2.0 is used to handle payments they can be initiated with a plastic card, a smartphone, in a webstore etc. Messages are used to interact with the bank. The messages will often contain sensitive information like PIN codes, account numbers, amounts etc. and needs to be secured (encrypted and signed).

The BALTUS 2.0 infrastructure is a secure network that can be used to forward messages from the service specific infrastructure at vendors or merchants (AO) and provide accesses to the banks (AO). In order to send a message through BALTUS 2.0, the originated service (for example a Bank-Axept card payment) and the requested bank destination (AO) must correspond with the BALTUS 2.0 routing table (LRM). The node operator role (NOP) will act as a BALTUS 2.0 "gatekeeper" and deliver valid messages to the appropriate receiving node. The receiving node receives the message and verifies the legitimacy based on the LRM functionality and a BALTUS 2.0 blacklists (Controlled by Finans Norge). After the verification, the node operator forwards the message to the appropriate destination (AO). The whole operation normally takes about half a second.

The Central Routing Table (CRT) contains all valid entities and services that can use the network. Finans Norge are responsible for validating entries to the CTR both entities and services.

Model describing the principles of BALTUS 2.0:



Solution and benefits

The requirements for BALTUS 2.0, designed to fulfil the defined quality requirements given by the BSK board, are listed below:

TRUST AND SECURITY

Some security requirements are linked to individual services, others constitute fundamental BALTUS security.

- **Confidentiality:** Prevent illegitimate or unwanted access to data, Introduce application to application security (end to end).
- **Integrity:** Prevent unwanted manipulation of data.
- **Control of Services:** Make sure that only approved service applications can generate transactions in the infrastructure.

FLEXIBILITY

- No dependencies to specific hardware or software.
- Message and transportation is two separated mechanisms. A new service can be introduced without any need for redesigning the infrastructure. Ditto for new messages/standards.
- Standardized routines for introducing new nodes, services, and ICT vendors. E.g. in order to ensure healthy competition provide documentation and routines so that new ICT vendors might enter the infrastructure in a controlled way.

EFFICIENCY

Provide cost effective and reliable services.

- Share cost and collaborative governance to ensure efficiency.
- Scalable capacity for future demands.
- Load balancing, no bottlenecks in the network and routing of messages the shortest way.
- Proactive maintenance, yearly risk assessment, BALTUS 2.0 Forum, Certification process defined.

AVAILABILITY AND ROBUSTNESS

- Avoid single point of failures to ensure end-to-end 100% availability.
- Simplification of complexity.
- Robustness against interference from uncontrolled threats or human errors.
- Routines and capability to handle unwanted incidents, Control and means for minimizing the consequence.
- Stop/blocking of nodes and services that is suspicious/threatening.
- Certification of Node operators.

What's in it for the business?

BALTUS 2.0 will provide the banks with a:

- Platform that can be utilized as part of the total business architecture to support new services/messages. It will reduce the time to market for new "cross-bank-services".
- Potential for more efficient and healthier competition in the market for ICT services since new node operators can get access to the new infrastructure for BALTUS 2.0.
- Reliable, stable and trustworthy offerings of services. BALTUS 2.0 is designed for high availability and stability, and the architecture procedures are designed for fast recovery.
- Flexible infrastructure that supports the transactions with a high degree of security and confidentiality. Further it will ensure that only compliant services will be accepted in the BALTUS 2.0 infrastructure.
- Technology neutral infrastructure that enables the banks to make use of new technology when relevant.

Information

Do not hesitate to contact BSK if you want more information:

✉ post@bsk.no

💻 www.bsk.no