Detailed Description of STRIDE and LINDDUN for E-Voting

STRIDE is a framework developed by Microsoft that is used as a mnemonic for the following security threat categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges. It generally applies to any IT infrastructure, specifically for scenarios with large attack surfaces (such as Internet voting). However, in the case of e-voting systems, the *information disclosure* category does not enable the identification of all types of attacks on privacy that the voter or the system can suffer.

LINDDUN is a privacy-oriented framework that considers the following privacy threat categories: Linking, Identifying, Non-Repudiation, Detecting, Data Disclosure, Unawareness and Unintervenability, and Non-Compliance. It aims to model risks associated with the links established between individuals and the data they generate. Of particular interest for the e-voting scenario are *linking* and *identifying*. These pose an inherent risk to any voting system, electronic or otherwise, in which voters must be authenticated as having the right to vote and uniquely distinguished from other voters, but the expression of their voting intentions must be unlinkable with their identities while being tallied and published in the final aggregate.

The following list reports the threat categories from STRIDE and LINDDUN, adapted to the context of e-voting.

Spoofing (SP): pretend to be a trustworthy entity to gain unauthorized access to sensitive data. For instance, impersonate a voter (e.g., by gaining access to their device) to vote for a different candidate, or an authority service to intercept a voter's request for the anti-coercion credentials.

Tampering (TA): maliciously change or modify data stored or in transit. This can be performed on any of the communication channels or by compromising one of the web servers or the voters' devices.

Repudiation (RE): perform prohibited operations without leaving traces. In the context of e-voting this translates to violating the verifiability of the system. More precisely, a repudiation attack manages to conceal evidence that a forbidden action has been performed or that some task has not been executed correctly; while the verifiability required from an e-voting systems prescribes that it is possible to check the correct execution of the protocol.

Information disclosure (ID): read data stored or in transit without the necessary permissions. This results in leaking sensitive data, e.g., by compromising one of the entities or listening on communication channels.

Denial of Service (DS): deny access to resources, such as by making a web server temporarily unavailable or unusable.

Elevation of privilege (EP): gain privileged access to resources in order to gain unauthorized access to information or to compromise a system.

Linking (LN): associate data items or voter actions to learn more about a voter or groups of voters. For instance, by associating a voting credential with the identity of a voter.

Identifying (IF): learn the identity of a voter, for instance in case of compromising a voter's device.

Non-Repudiation (NR): being able to attribute an action to a voter, for instance in case of an over-the-shoulder attack. This is the core threat category for coercion scenarios.

Detecting (DT): deduce the involvement of a voter through observation, e.g., while listening on the communication channel between the voter's device and the web servers. This threat category is also crucial in coercion scenarios.

Data Disclosure (DD): excessively collect, store, process, or share voters' personal data.

Unawareness and Unintervenability (UU): when individuals are not sufficiently informed, involved, or empowered concerning processing of their personal data.

Non-Compliance (NC): when the system deviates from legislation, regulation, or from standards and best practices.