Trust Model Glossary

These terms are used in DTI's *Trust Model* and other data portability trust work.

Trust Criteria

A set of standards used by Transfer Parties to evaluate and establish trust to facilitate direct data transfers.

Artifact

An attestation or materials that may be useful in demonstrating each Trust Criteria. These may be verifiable, certified by a third party, self-certified, simple attestations, or other variations.

CSAM or Content Moderation Program

A Transfer Party program reviewing and monitoring user-generated content to ensure that it meets certain standards and guidelines.

Data (Information)

General terms that could describe many different types of people's information.

Data Portability

Users' ability to download and transfer personal data they have contributed to services along with data reflecting their activity within services.

Data Transfer

The action of copying the data type and moving the copy to the destination.

Denial of Service

The threat that a Transfer Party service becomes inaccessible or overloaded due to a flood of requests or data.

Elevation of Privilege

The threat that attackers try to gain access to to Transfer Party system resources they are not entitled to often through unexpected means (e.g., overflow buffers).

End User

The individual seeking to transfer their data from one provider (Sender) to another provider (Reciever). This may include an individual acting on behalf of a business

Harmful Content

Content that is, or can be, harmful to the service, the End User, or to other users.

Inadequate Transparency

The threat that a Transfer Party may not provide adequate public or End User transparency regarding its data processing practices.

Non-Compliance

The threat that a Data Transfer between two Transfer Parties does not comply with laws, regulations, or Data Transfer Party policies.

Unanticipated User Processing Permissions

The threat that Transfer Data will not have the expected or appropriate permissions or access control after Transfer to the Receiving Party.

Processor

A party, who is not a Transfer Party, but who processes End User data on behalf of a Transfer Party.

Receiving Party

A type of Transfer Party that receives a Data Transfer. A transfer party may be a Sender, Receiver, or both. May also be referred to as “Receiver.”

Repudiation

The threat that a Sending Party or the End User may deny that content was posted or that it was posted by the user, or that the metadata is inaccurate. This is largely mitigated by using secure transport.

Sending Party

A type of Transfer Party that sends a Data Transfer. A Transfer Party may be a Sender, Receiver, or both. May also be referred to as “Sender.”

Service

Generic term that encompasses apps, websites and companies.

Spoofing

The threat that a Data Transfer participant convinces a Transfer Party in a data transfer that they are somebody else other than who they are.

Tampering

The threat that a Party who is not part of the Transfer modifying Transfer Data during the Transfer.

Transfer

The action of copying or sending End User data from the Sending Party to the Receiving Party.

Transfer Mechanism

The technical implementation of a Transfer.

Transfer Party

Term to encompass both Sender, Receiver, and User Agent parties within a transfer relationship

Trust Model

A set of criteria for Transfer Parties to assess trustworthiness as they mutually authorize each other for a direct transfer.

Trusted Relationship

Trust Registry

A trust registry is a centralized service that contains information that can be used to evaluate the trustworthiness of Transfer Parties.

Unauthorized Disclosure

The threat of exposure of Transfer Data in transit to an unauthorized Party. This can often be mitigated by using secure transport and technical authentication mechanisms.

Unauthorized Transfer

The threat of a transfer without End User authorization.