AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE
DEPARTMENT OF CYBERSECURITY AND CRYPTOLOGY

LEGAL REGULATION OF INFORMATION SECURITY

Lecturer: PhD, Acting Associate Professor Assem Turarbek

MODULE 1

INFORMATION SECURITY AND ELECTRONIC SERVICES

LECTURE 3

LEGALLY SIGNIFICANT ACTIONS IN INFORMATION SYSTEMS AND NETWORKS

LECTURE OBJECTIVE

Identify legally significant electronic actions and explain how authentication, digital signatures and records help establish identity, consent and the content of an agreement.

LECTURE PLAN

1. Electronic transactions and written form

2. Digital signatures and identity verification

3. Validity and evidence in electronic disputes

LEGAL EFFECTS OF AN ELECTRONIC ACTION

Concept or participant	Meaning, duties and application
Transaction	An act intended to create, change or terminate civil rights and obligations.
Unilateral transaction	The will of one party is sufficient where the law or an agreement permits it.
Contract	Two or more parties express agreement. Online purchases and service contracts are common examples.
Service interaction	Opening an account, accepting terms and submitting a service request may have different legal effects.

A user may enter several relationships during one online interaction, including a communications service, a platform agreement and a particular order. Each relationship has its own parties and terms. Identifying the relevant transaction prevents confusion between account registration, permission to use the platform and agreement to a specific paid service.

WRITTEN FORM IN AN ELECTRONIC ENVIRONMENT

Concept or participant	Meaning, duties and application
Electronic documents	A written transaction can take electronic form where the applicable rules permit it.
Exchange of messages	A document exchange can evidence agreement when the parties can be identified and the content of their agreement can be determined.
Applicable conditions	The law or the parties' agreement may prescribe a particular form or method of signing.

The retained document needs to establish what the parties agreed to. Readability, identification of the parties and preservation of the content are therefore significant. When terms change over time, the version associated with the acceptance event matters. A general copy of today's terms may differ from those shown during the earlier transaction.

ELECTRONIC DIGITAL SIGNATURE

Concept or participant	Meaning, duties and application
Signer	The signer applies an electronic digital signature (EDS) to the document.
Verification	The recipient verifies the signature and checks whether the certificate links the signing key to the claimed signer.
Integrity	Verification helps establish whether the signed content has changed since signing.
Authority	The identity of the signer and the signer’s authority to act for another party are separate questions.

The certification authority supplies an identity link through the certificate. Verification of a signature also depends on the signed content and the applicable certificate checks. Representation adds another question, because the person signing for an organization needs authority for that action. Identity evidence and evidence of authority serve different purposes.

IDENTIFICATION AND CONSENT BY ONE-TIME CODE

Registered number

A public electronic resource may associate the user with a registered mobile number.

One-time password

A short-lived SMS code can verify control of that number for a specific interaction.

Agreement record

The service can retain the version of the terms presented to the user and the time and outcome of confirmation.

The one-time code forms part of a specific interaction with the service. A useful record associates the confirmation with the number, account, request and terms presented at that moment. It also records the outcome and time. This association matters if the user later disputes which action the confirmation concerned.

ELECTRONIC EVIDENCE IN A DISPUTE

Identity

Account records, certificate information and authentication records can help establish who acted.

Content

The signed document or retained message shows the terms, instruction or declaration at issue.

Timing

A timestamp, delivery record or system log can establish when the action occurred.

Integrity

The credibility of a record depends in part on how it was stored and whether changes can be detected.

Electronic evidence is stronger when separate records support the same account of events. For example, an accepted order can be compared with the payment record, the signed document and the delivery record. Inconsistent times or missing steps need explanation. The organization’s retention and access arrangements affect the completeness of this reconstruction.

TRANSACTION VALIDITY

Form and permission

A missing authorization, expired permission or failure to meet a required form may affect validity.

Capacity and authority

The parties’ legal capacity and a representative’s authority matter.

Consent

Material mistake, fraud, duress or collusion may affect whether the transaction is valid.

Legal consequences

The legal effect and available remedies depend on the grounds and the applicable procedure.

The source lists circumstances involving permission, capacity, significant mistake, deception, pressure and representative misconduct. Assessing one of these grounds requires the surrounding circumstances and the applicable legal procedure. A record of successful authentication establishes part of the interaction, while the validity question also concerns the person’s authority and expression of will.

ELECTRONIC INTERACTION ACROSS BORDERS

UNCITRAL Model Law on Electronic Commerce

A framework for recognizing electronic records and assessing whether they fulfil the functions of written documents.

ISO/IEC 27001

A management system standard for information security. It provides a framework for managing controls around electronic records.

Cross-border electronic interactions can involve different rules about form, recognition and evidence. A model law supports harmonization, while an information security management standard concerns the organization’s management of security. When evaluating an electronic record, the relevant legal rules and the technical controls around its creation and retention both matter.

CASE DISCUSSION

A user disputes accepting an online service agreement. The provider has a successful SMS verification record and a time of login.

Which records could establish what the user agreed to and when?

What would change if the record contained the signed document and its certificate details?

Analysis

The agreement text, version identifier and time of acceptance would connect the terms to the event. A valid signature can support identity and integrity checks. Validity also depends on the applicable form, authority and consent requirements.

ELECTRONIC AGREEMENT AND EXPRESSION OF WILL

The lecture describes unilateral transactions and contracts involving two or more parties. A contract requires evidence of agreement on its content. In an electronic environment, the retained record connects the parties with the terms they accepted.

A message exchange can serve this function when the sender and recipient can be identified and the content remains readable. The applicable law or agreement can prescribe a specific form, signature or verification method.

A certification authority links a public key to the identity recorded in a certificate. Verification checks the signature against the signed content and the associated public key.

The reviewer also considers certificate validity and the authority of the signer. For an organization, identifying an employee does not by itself establish that the employee was authorized to conclude that particular transaction.

GROUNDS AFFECTING TRANSACTION VALIDITY

The source discusses missing permission, capacity limitations, material mistake, deception, threats and improper conduct by representatives. These circumstances concern the validity of consent or the authority to act.

The legal effect depends on the specific ground and procedure. A dispute about a transaction requires examination of both the agreement and the surrounding evidence, including identity records and the information presented to the parties.

A provider can preserve the accepted terms, document version, time of acceptance, authentication outcome and subsequent service actions. These records help reconstruct the interaction.

A useful investigation compares the application record with independent sources such as message delivery, signature verification and payment records. Differences between clocks, missing events and later changes to records affect interpretation.

CONCLUSION

1. Electronic records can establish the parties, the terms and the timing of an action.

2. Digital signatures help verify the signer and the integrity of a document.

3. Validity also depends on the applicable form, authority and consent requirements.

SELF-ASSESSMENT QUESTIONS

1. What makes an electronic action legally significant?
2. How can identity, authority and consent be established in an electronic transaction?
3. What functions does a digital signature perform?
4. What records help establish the content and timing of an electronic agreement?
5. Why does a valid digital signature alone not resolve every question about a transaction’s validity?

REFERENCES

1. Lecture 3. Legally Significant Actions in Information Systems and Networks. Course materials.

2. UNCITRAL. Model Law on Electronic Commerce.

3. ISO/IEC 27001. Information security management systems.