CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Keamanan dan Pengelolaan Data

Minggu 2

Dosen Pengajar: Steven Bandong S.Si., M.T

Tata Tertib Kelas

- Dosen dan mahasiswa bersama-sama secara aktif membentuk komunitas belajar yang baik
- Silahkan bertanya kalau ada yang tidak dimengerti
- Laporan / program / tugas apa pun yang anda serahkan harus jelas beda dan jelas adalah kontribusi anda atau kelompok dan bukan dari orang lain (misnya: tugas proyek).

Topik Minggu Ini dan Capaian Pembelajaran

Topik minggu ini:

1. Menjelaskan empat jenis algoritma kriptografi.
2. Memahami konsep infrastruktur kunci publik.
3. Menjelaskan konsep privasi

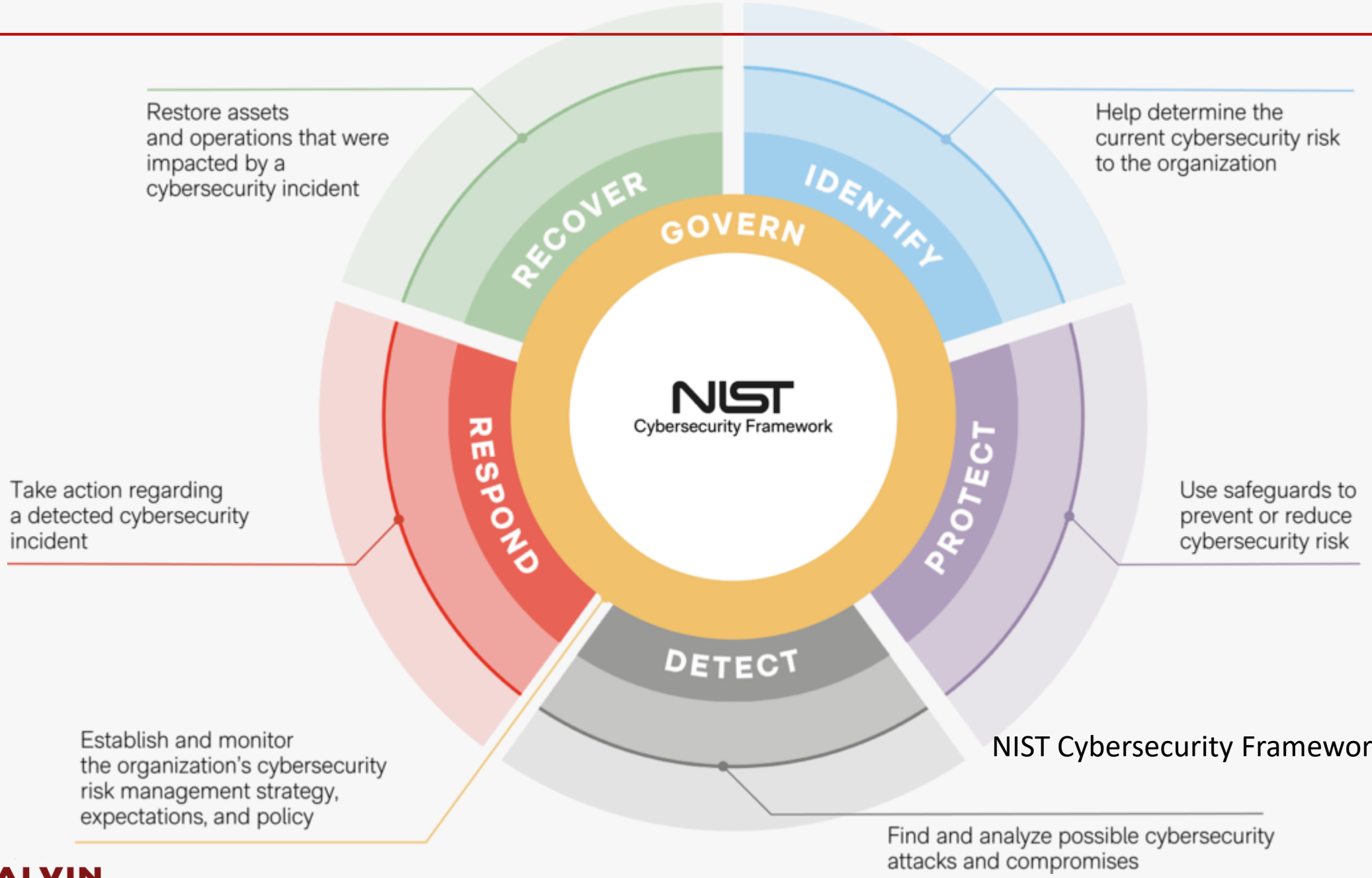
Indikator penilaian:

1. Ketepatan dalam menjelaskan empat jenis algoritma kriptografi
2. Ketepatan dalam menjelaskan infrastruktur kunci public
3. Ketepatan dalam menjelaskan konsep privasi

NIST Cybersecurity Framework

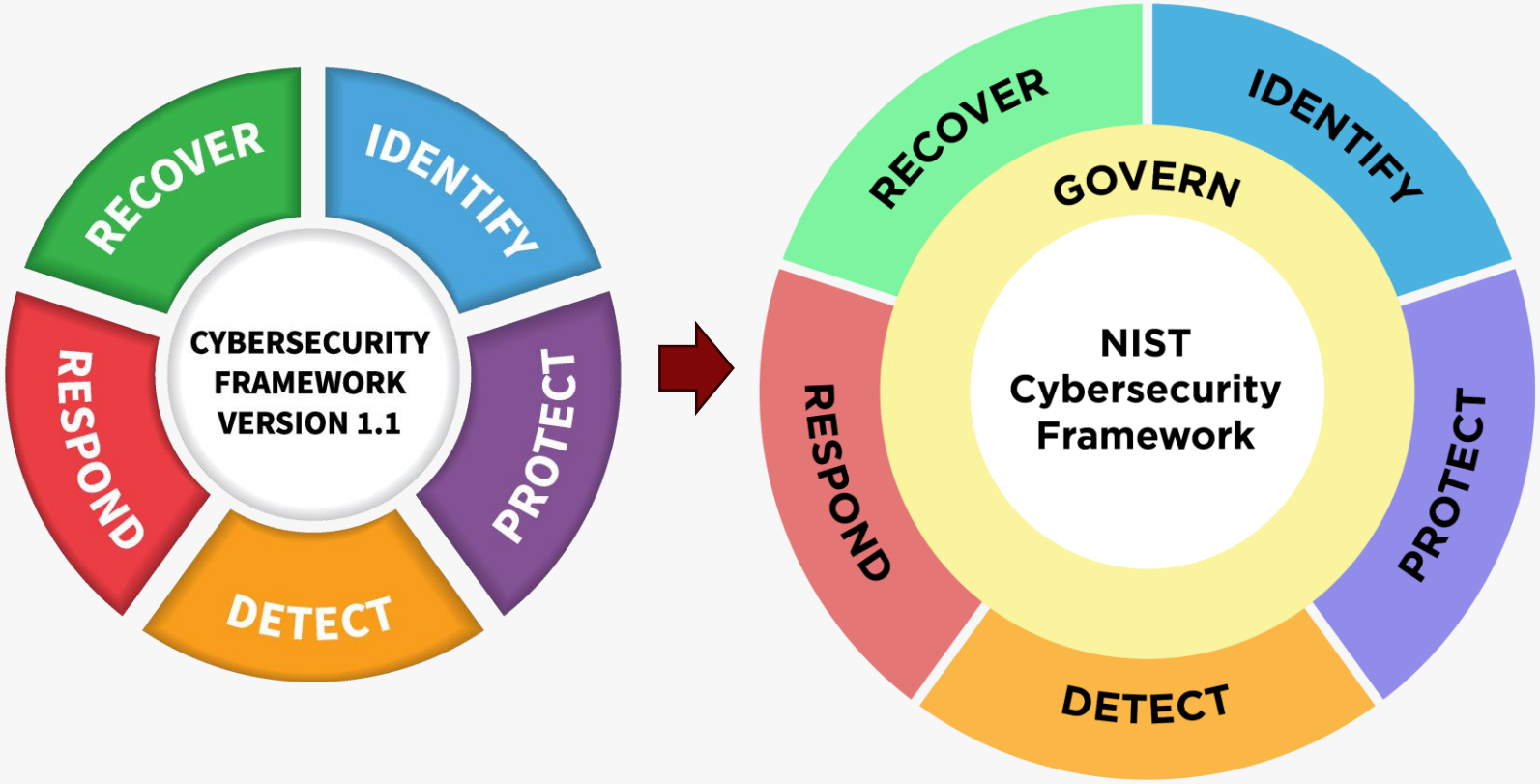
NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communication	Improvements
Governance	Data Security	Detection Processes	Analysis	Communication
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



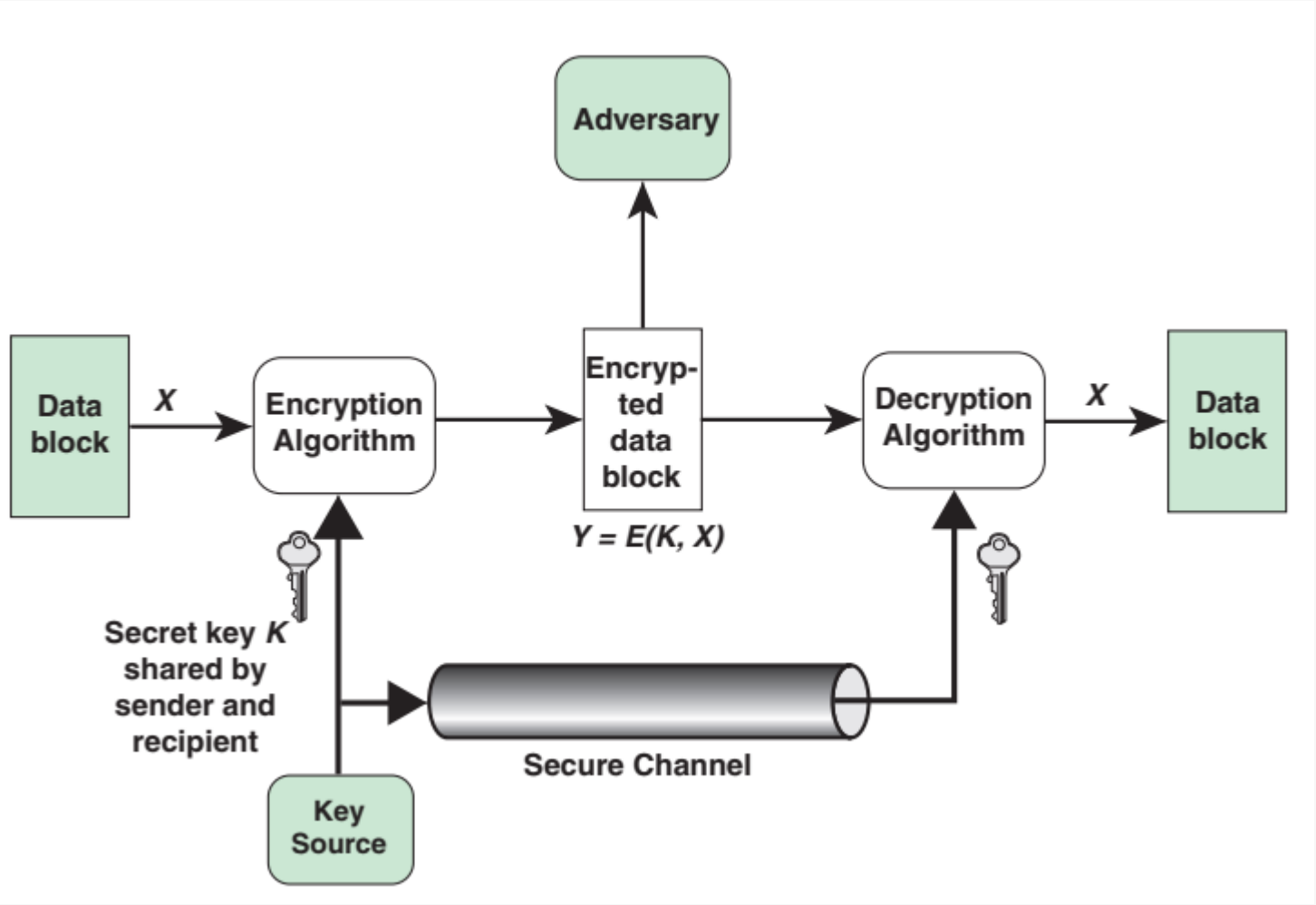
NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework

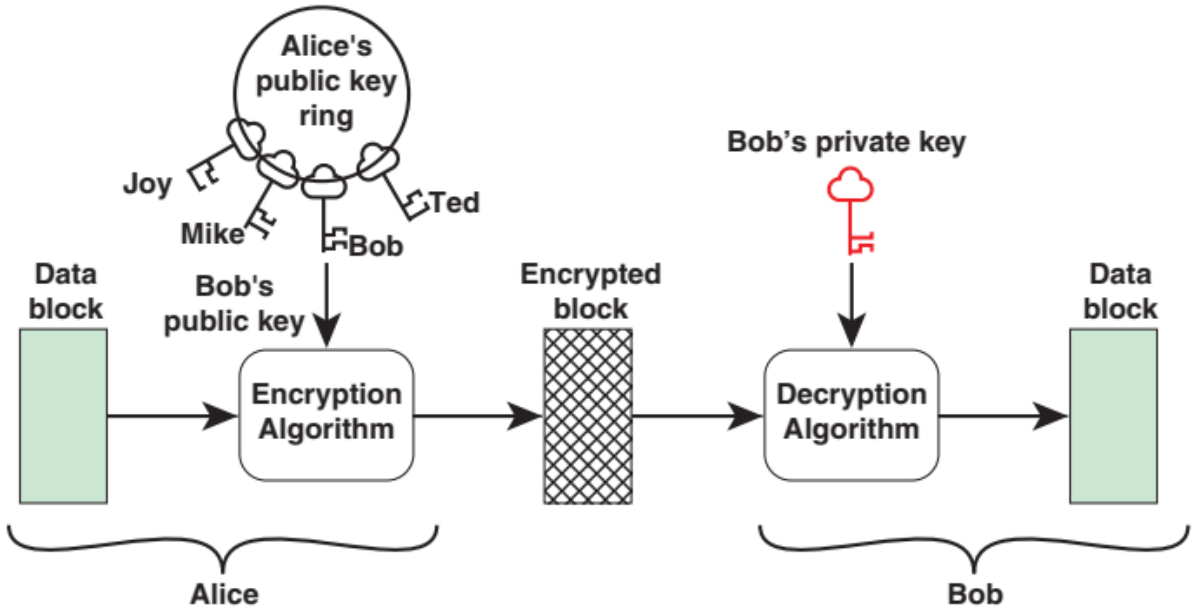


Apakah menjawab objektif Cybersecurity?

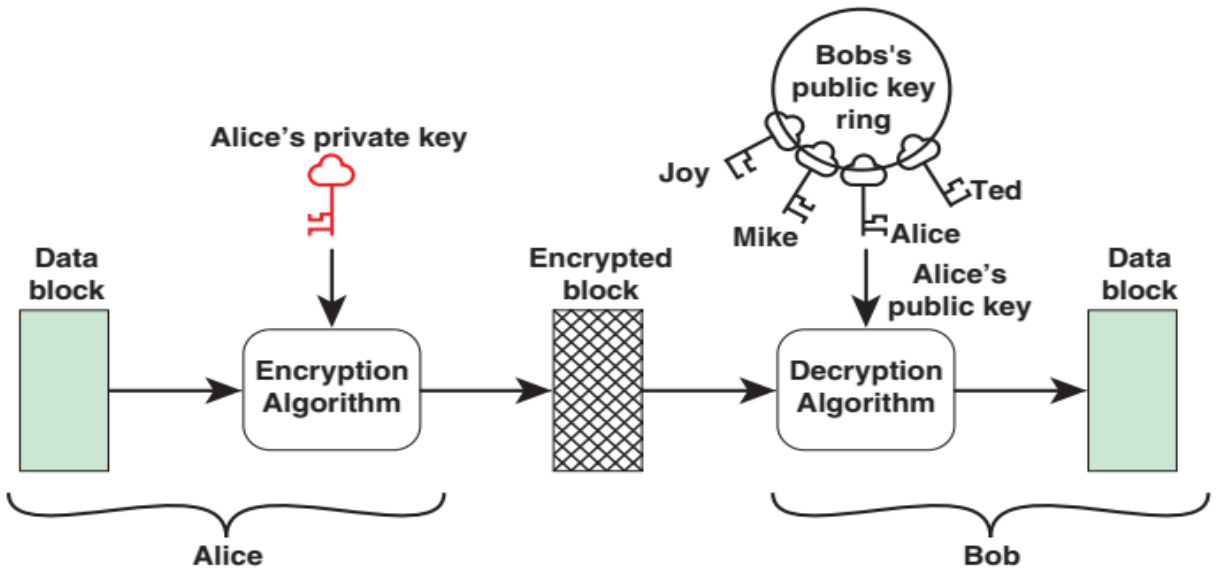
Symmetric Encryption



Asymmetric Encryption



(a) Public-key encryption/decryption (Alice encrypts block for Bob only)



(b) Public-key encryption/decryption (Alice authenticates block for any recipient)

Practical Considerations

Keamanan Kriptografi
Keamanan Kriptografi bergantung pada pemilihan algoritma dan panjang kunci yang tepat.

Panduan:
FIPS 140-2A (Approved Security Functions for FIPS PUB 140-2)
SP 800-131A (Transitioning the Use of Cryptographic Algorithms and Key Lengths)
ENISA Algorithms, Key Size and Protocol Report.

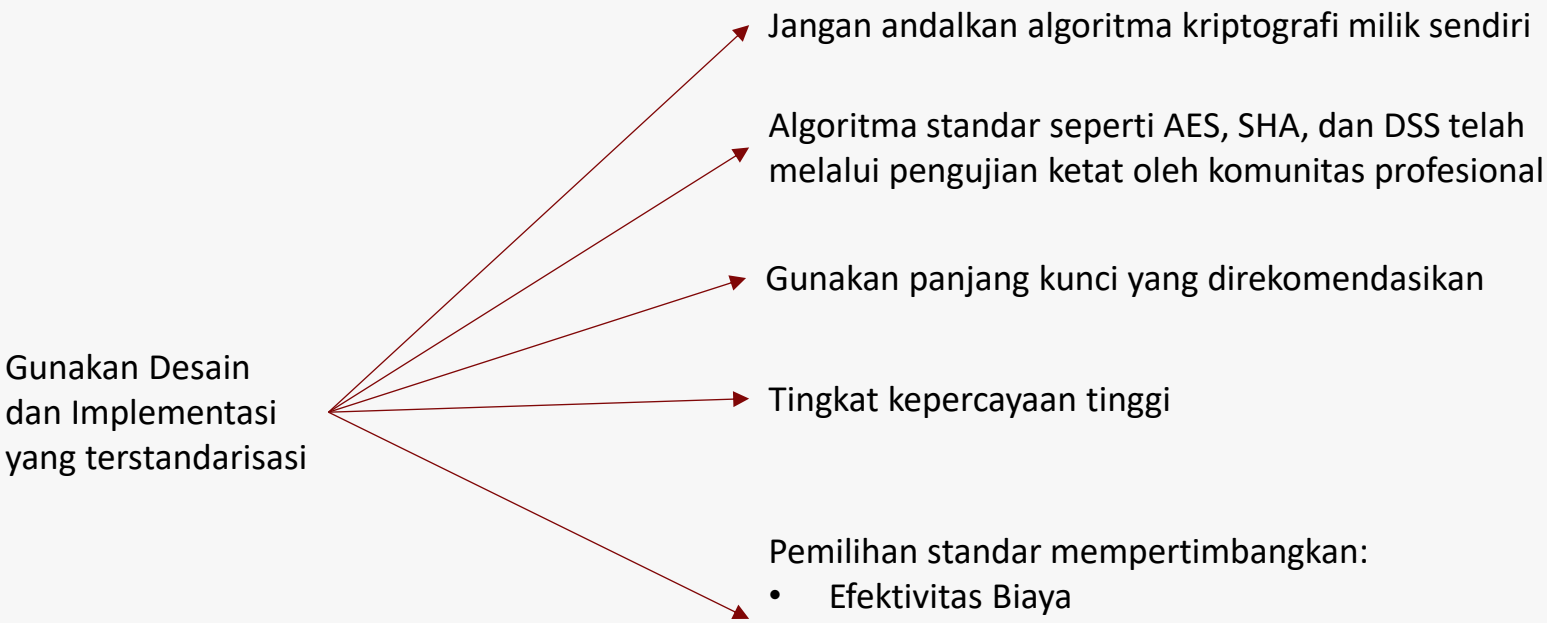
Rekomendasi NIST:
Enkripsi Simetris: Algoritma enkripsi Advanced Encryption Standard (AES) dengan panjang kunci 128, 192, atau 256 bit.
Hash Function: SHA-2 atau SHA-3, dengan panjang hash antara 224 hingga 512 bit. SHA-3 melengkapi SHA-2 tetapi tidak menggantikannya.
Digital Sign:

- DSA dengan kunci 2048-bit.
- RSA dengan kunci 2048-bit.
- Elliptic Curve DSA dengan kunci 224-bit.

SP 800-131A juga mencakup rekomendasi untuk algoritma *generator random* bit, kode autentikasi pesan, algoritma *agreement key*, dan algoritma enkripsi kunci.

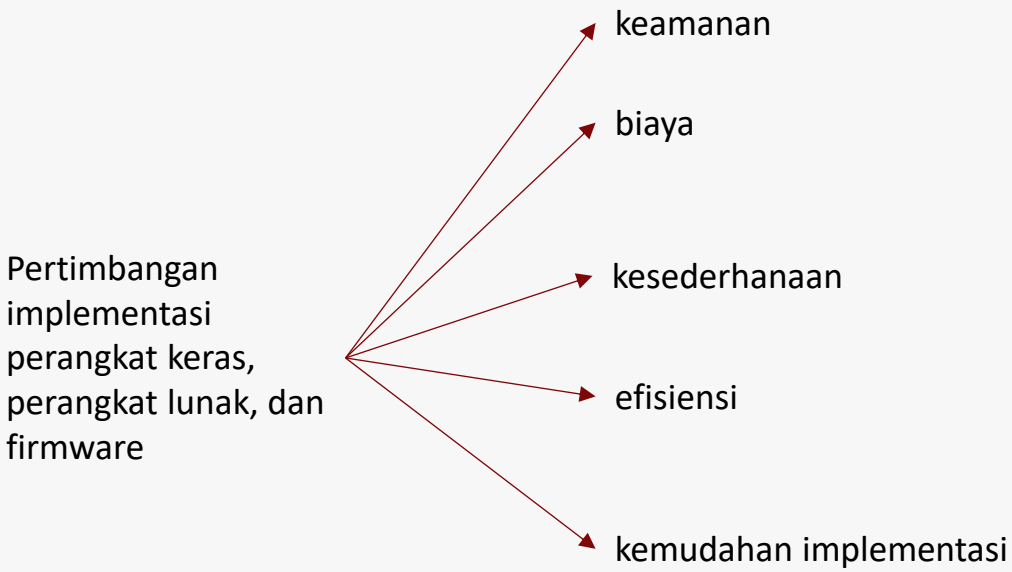
Implementation Considerations

SP 800-12 (An Introduction to Information Security) memberikan pertimbangan penting untuk mengimplementasikan kriptografi dalam sebuah organisasi.



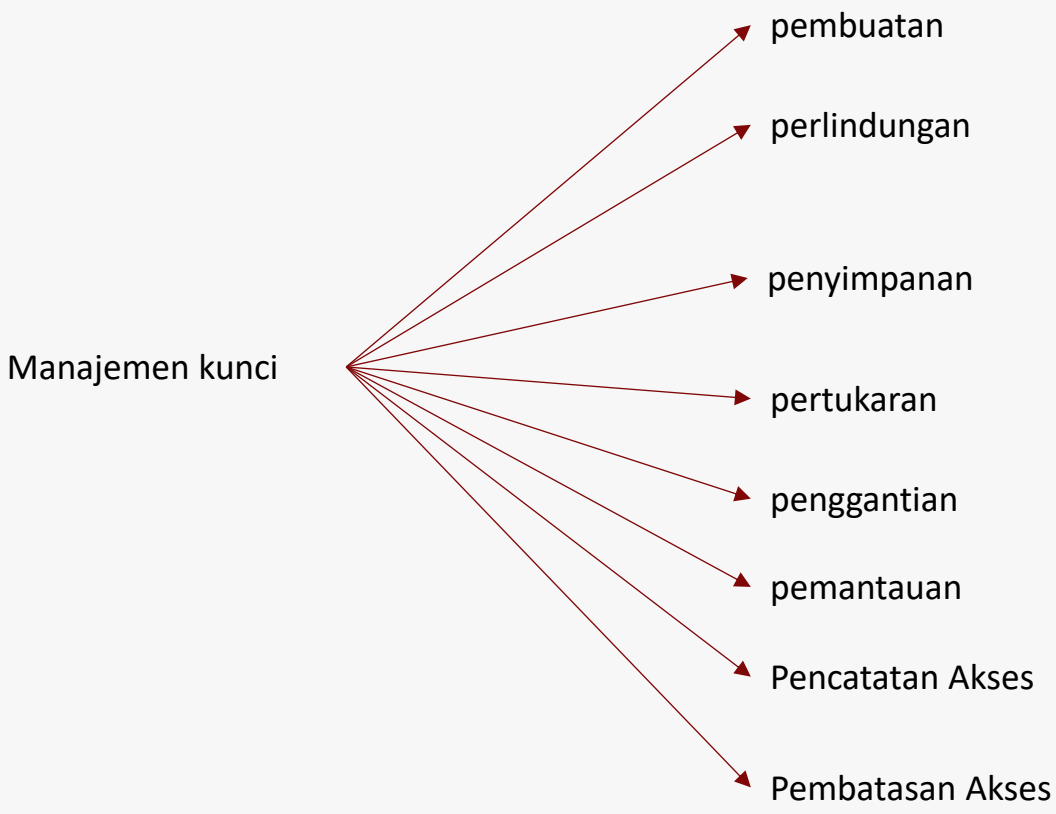
Implementation Considerations

SP 800-12 (An Introduction to Information Security) memberikan pertimbangan penting untuk mengimplementasikan kriptografi dalam sebuah organisasi.



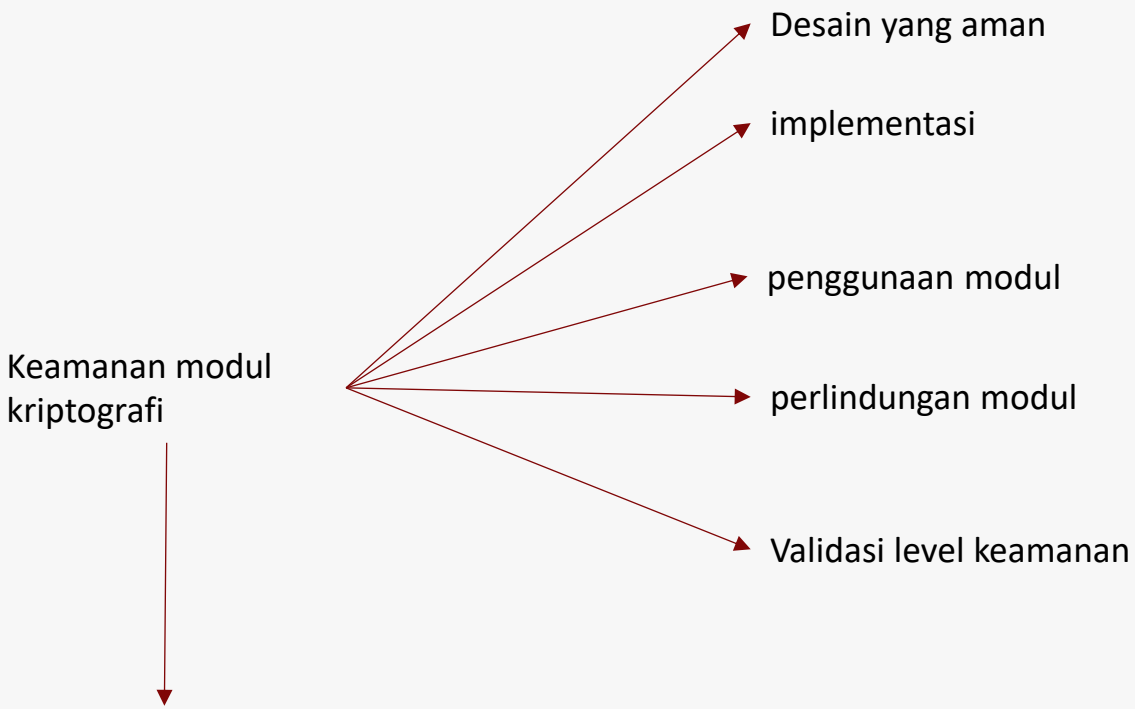
Implementation Considerations

SP 800-12 (An Introduction to Information Security) memberikan pertimbangan penting untuk mengimplementasikan kriptografi dalam sebuah organisasi.



Implementation Considerations

SP 800-12 (An Introduction to Information Security) memberikan pertimbangan penting untuk mengimplementasikan kriptografi dalam sebuah organisasi.



Modul kriptografi berisi algoritma kriptografi, parameter kontrol tertentu, dan fasilitas penyimpanan sementara untuk kunci yang digunakan oleh algoritma

Recent Advances

Lightweight Cryptographic Algorithms

Pengembangan algoritma yang tetap aman namun memiliki waktu eksekusi, penggunaan memori, dan konsumsi daya yang minimal

- Cocok untuk Embedded System & IoT
- Fokus pada Kriptografi Simetris dan Fungsi Hash
- **NISTIR 8114 (*Report on Lightweight Cryptography*)**

Post-Quantum Cryptographic Algorithms

Muncul akibat kekhawatiran bahwa komputer kuantum dapat memecahkan algoritma kriptografi asimetris yang saat ini digunakan

Artificial intelligence (AI) in cybersecurity menggunakan pembelajaran mesin dan jaringan saraf untuk meningkatkan keamanan jaringan, data, dan sistem komputer.

The Race Toward Post-Quantum Security Standards

The problem goes back to prime numbers. Although mathematicians have not found a way for traditional computers to efficiently break asymmetric encryption by calculating prime factors, they've discovered a way for quantum computers to do it — and they can do it very quickly.

The National Institute of Standards and Technology (NIST) is a government agency that helps set standards for technology. Lily Chen, who heads NIST's cryptographic technology group, said we will probably be dealing with the practical implications of quantum computers within 10 years.

"Experts predict that, around 2030, we'll have full-scale quantum computers that can break asymmetric key cryptography," Chen said. "So that will give us *some* time."

Researchers have already built quantum computers, although none precise and powerful enough to break the current standards. It's essentially a race now between the researchers working to improve the calculating power of quantum computers and those developing new encryption standards that can eventually hold up against those quantum computers. Chen said NIST is currently in the middle of a selection process for new, post-quantum security

https://builtin.com/articles/post-quantum-cryptography#:~:text=Although%20mathematicians%20have%20not%20found,can%20do%20it%20very%20quickly.

Public-Key Infrastructure

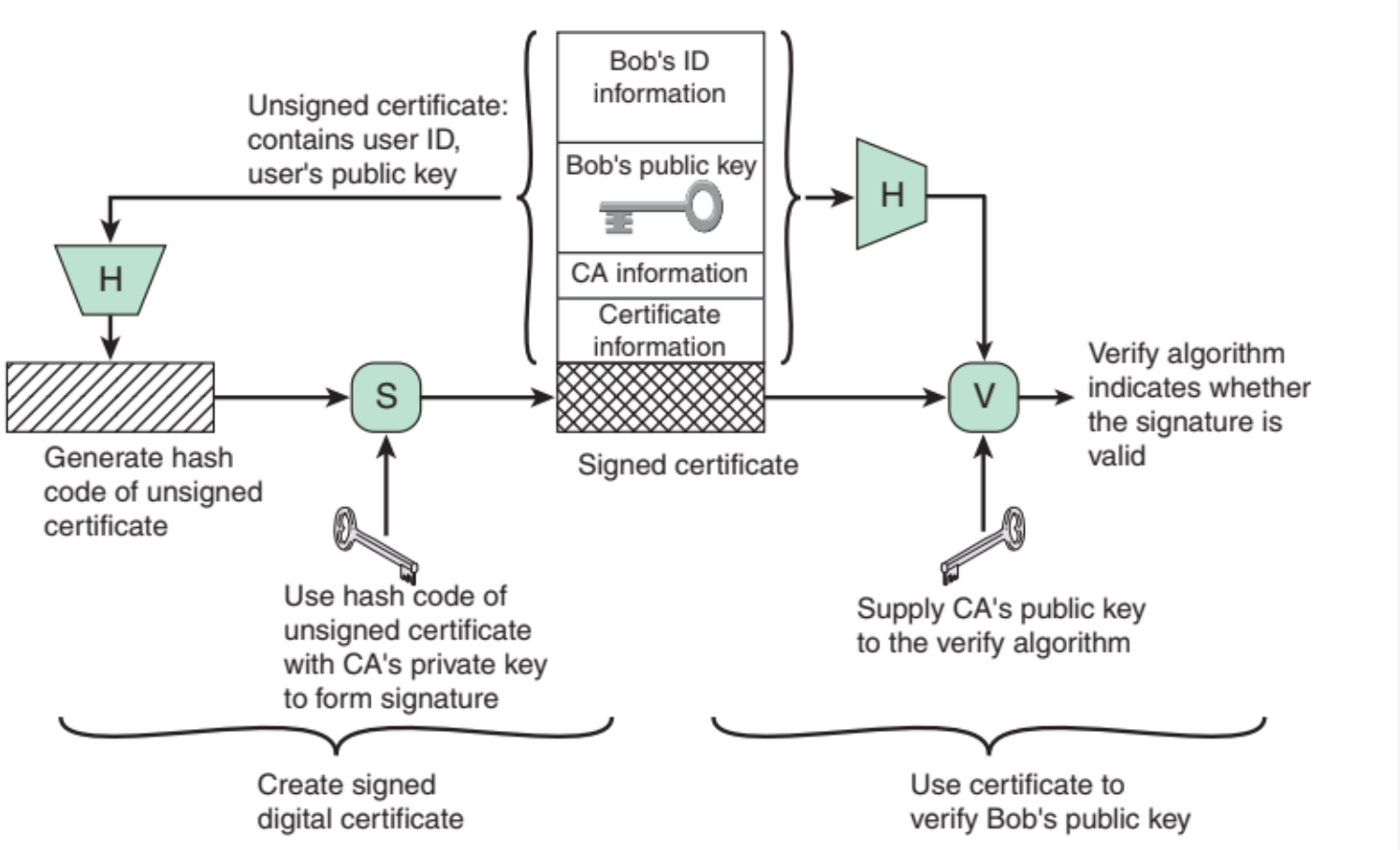
PKI mengatur pendistribusian dan pengelolaan kunci enkripsi publik untuk menjaga keamanan pertukaran data, memastikan identitas pengguna, dan memungkinkan verifikasi serta pencabutan sertifikat digital.

Public-Key Certificates

Public-Key Certificates adalah dokumen digital yang digunakan untuk mengidentifikasi seseorang/entitas. Sertifikat ini berisi kunci publik dan informasi penting lainnya, serta ditandatangani secara digital oleh pihak terpercaya, yaitu *certification authority* (CA), untuk memastikan bahwa kunci publik tersebut benar-benar milik pihak yang dimaksud.

Public-Key Certificates

Sertifikat Bob berisi identitasnya, kunci publik, dan detail dari CA, yang ditandatangani secara digital oleh CA. Sertifikat ini dapat disiarkan atau dilampirkan, dan keabsahannya diverifikasi melalui tanda tangan CA.



*The standard **ITU-T X.509** (The Directory: Public-Key and Attribute Certificate Frameworks) has become universally accepted for formatting public-key certificates.

PKI Architecture

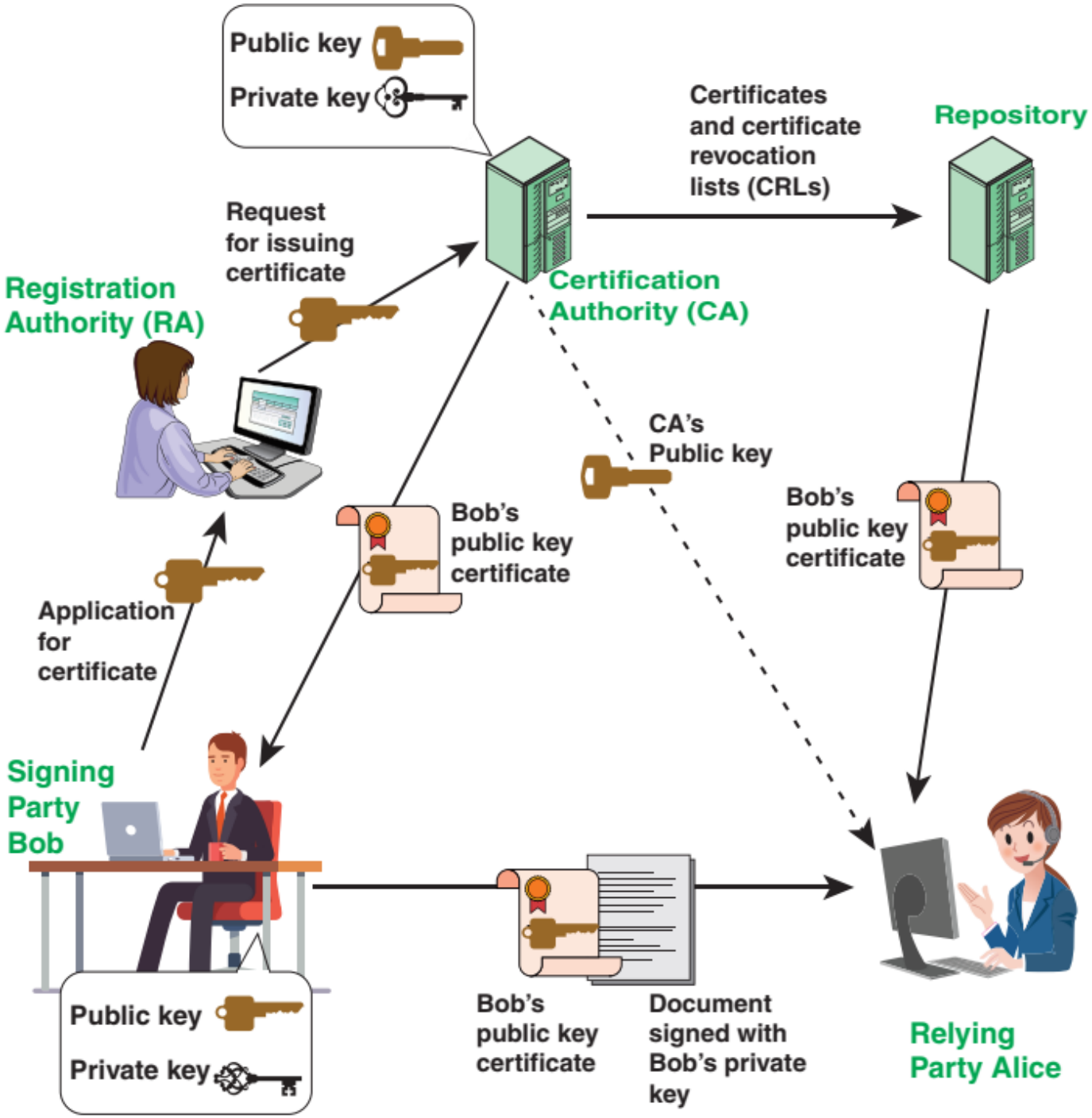
Arsitektur PKI mendefinisikan organisasi dan hubungan antar CA (Certification Authority) dan pengguna PKI. Arsitektur PKI harus memenuhi persyaratan berikut:

- Setiap peserta dapat membaca sertifikat untuk menentukan nama dan kunci publik pemilik sertifikat.
- Setiap peserta dapat memverifikasi bahwa sertifikat berasal dari otoritas sertifikasi dan bukan tiruan.
- Hanya otoritas sertifikasi yang dapat membuat dan memperbarui sertifikat.
- Setiap peserta dapat memverifikasi bahwa sertifikat saat ini masih berlaku.

PKI Architecture

Komponen-komponen penting PKI meliputi:

- Registration Authority (RA): Mengelola permintaan pembuatan sertifikat.
- Certification Authority (CA): Otoritas yang menerbitkan sertifikat kunci publik.
- Repository: Tempat penyimpanan sertifikat dan daftar pencabutan sertifikat (CRL).

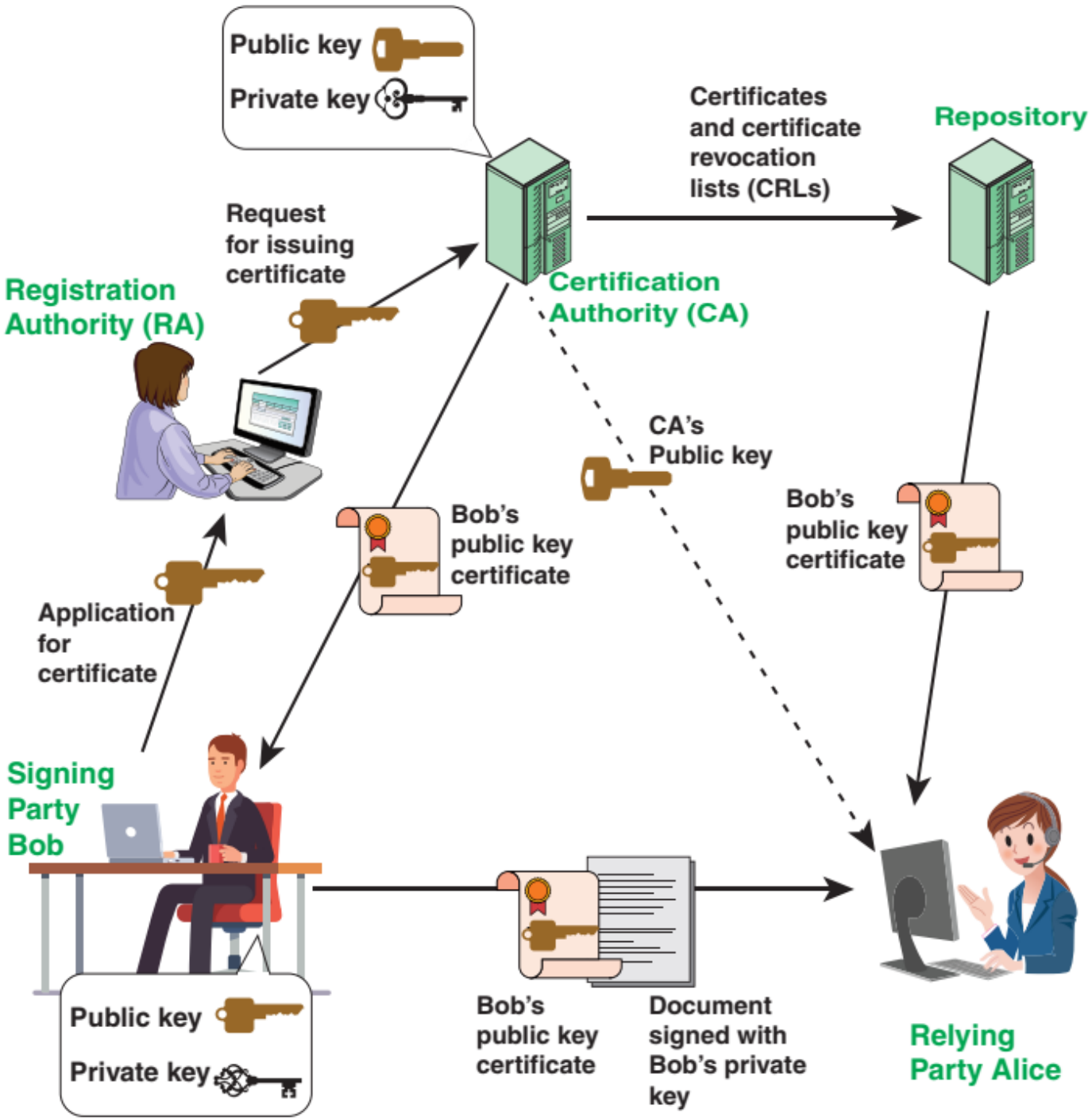


CALVIN INSTITUTE OF TECHNOLOGY

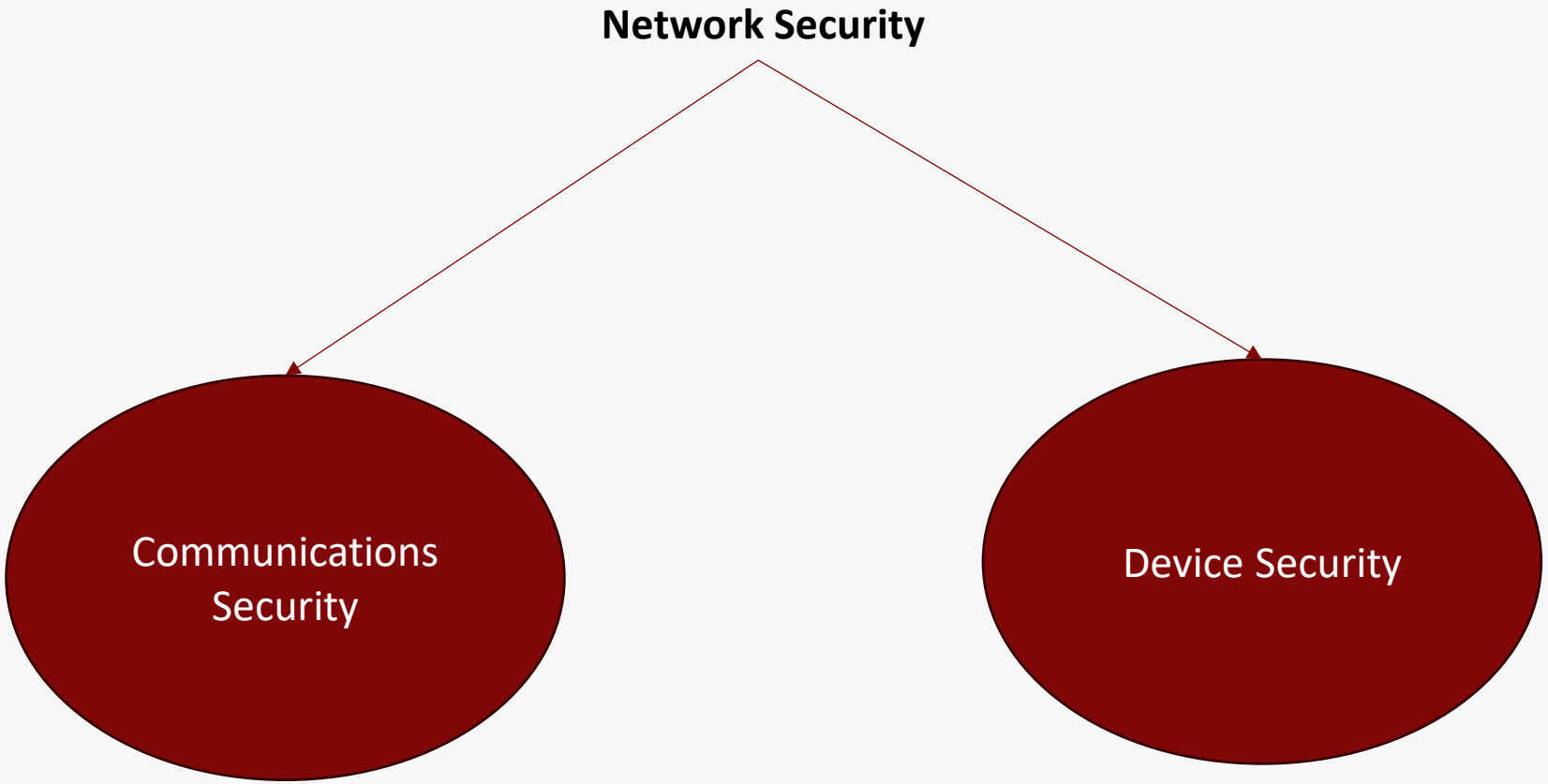
PKI Architecture

Proses PKI

- Bob mengajukan permintaan sertifikat ke RA.
- RA memverifikasi identitas Bob dan mengirimkan permintaan ke CA.
- CA menerbitkan sertifikat kunci publik untuk Bob, yang kemudian dapat didistribusikan.
- Sertifikat digunakan oleh Alice (pihak terpercaya) untuk memverifikasi dan menggunakan kunci publik Bob.

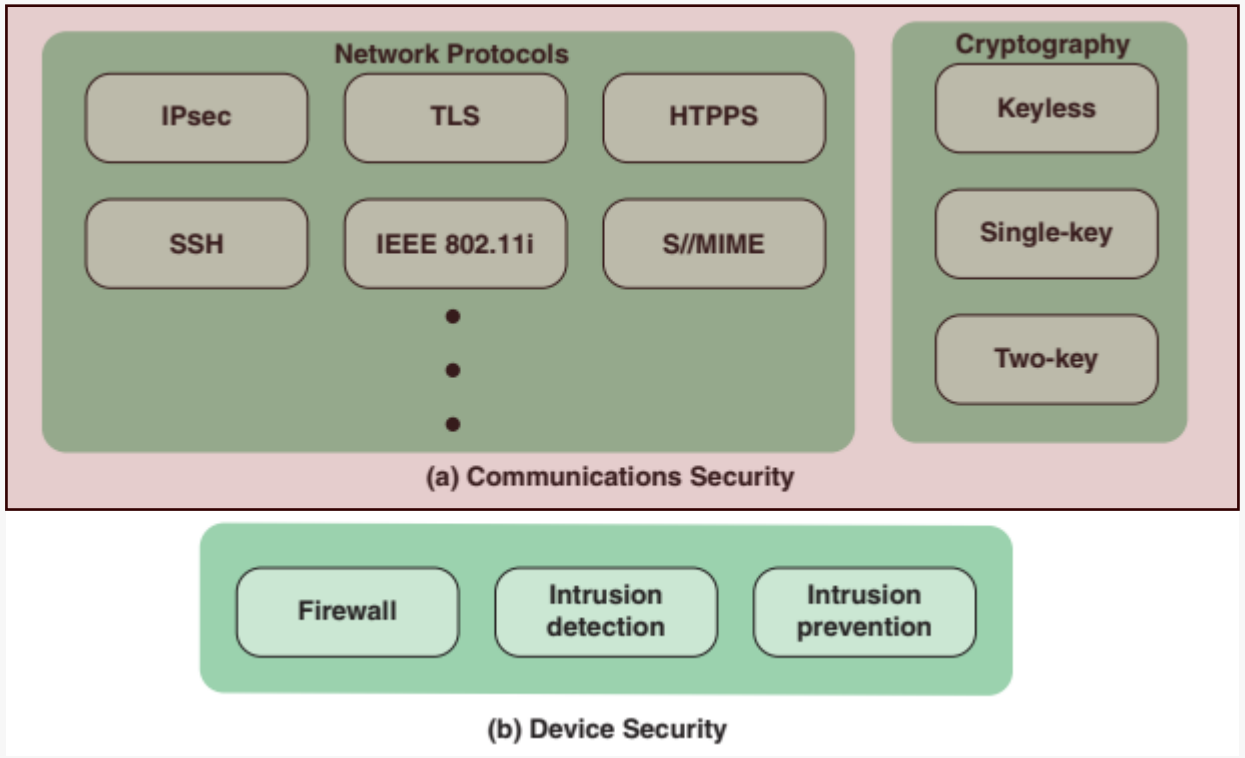


Network Security



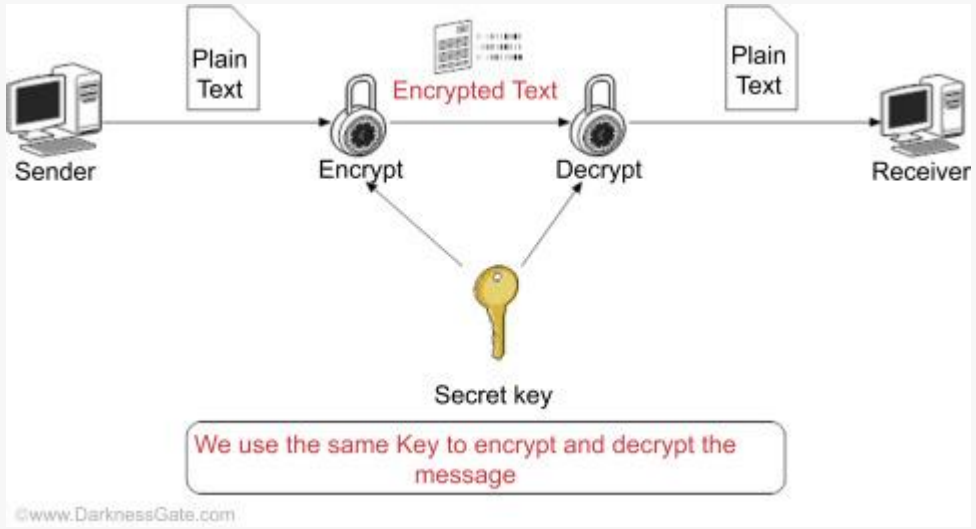
Communications Security

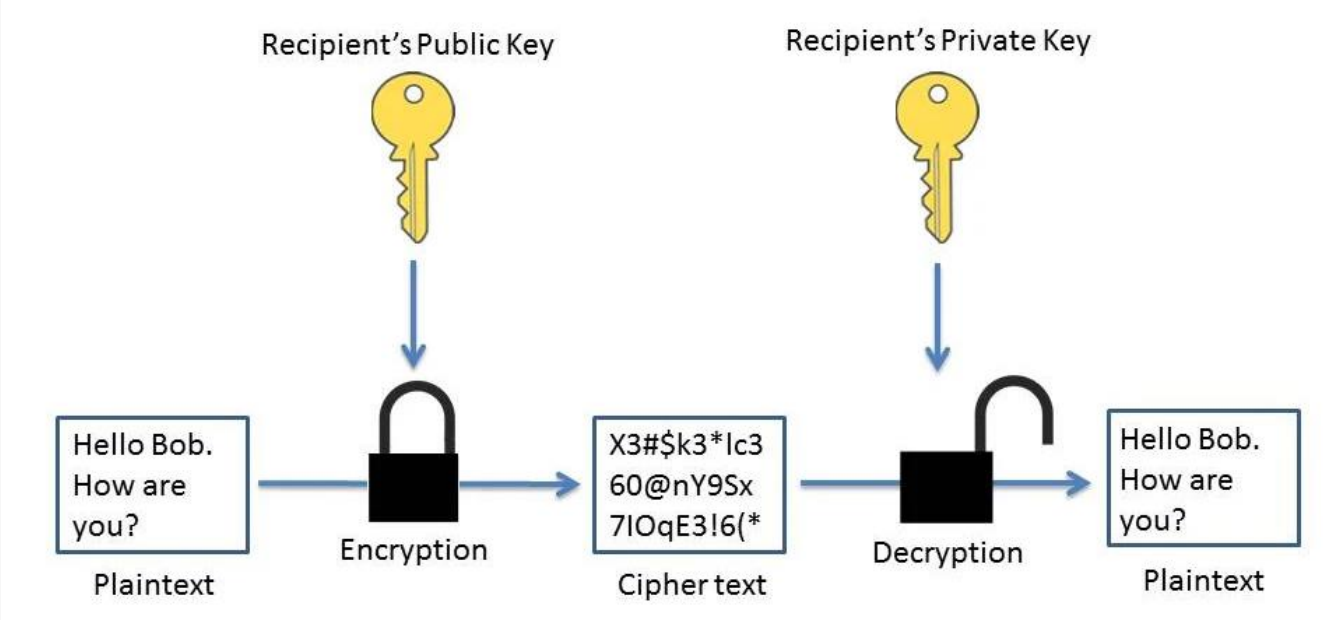
Keamanan komunikasi terutama menggunakan protokol jaringan untuk mengatur transmisi dan penerimaan data melalui format, struktur, dan kontrol transfer data.



Elemen kunci pada network security

Communications Security

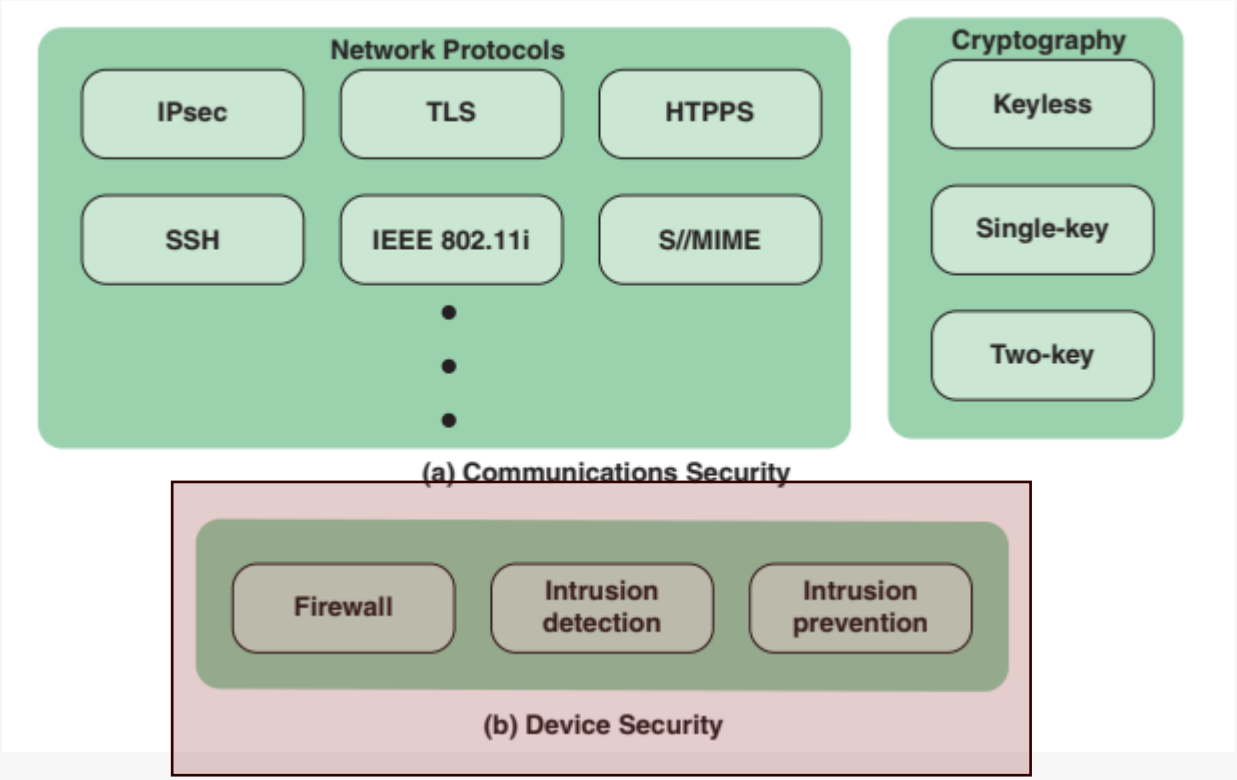




Device Security

Network security mencakup perlindungan perangkat (*device*) seperti router, switch, dan sistem klien/server dari penyusup, malware, dan beban berlebih yang dapat mengurangi availability sistem.

Firewall ➔ perangkat keras atau perangkat lunak yang membatasi akses jaringan dengan menyaring lalu lintas data berdasarkan aturan tertentu.

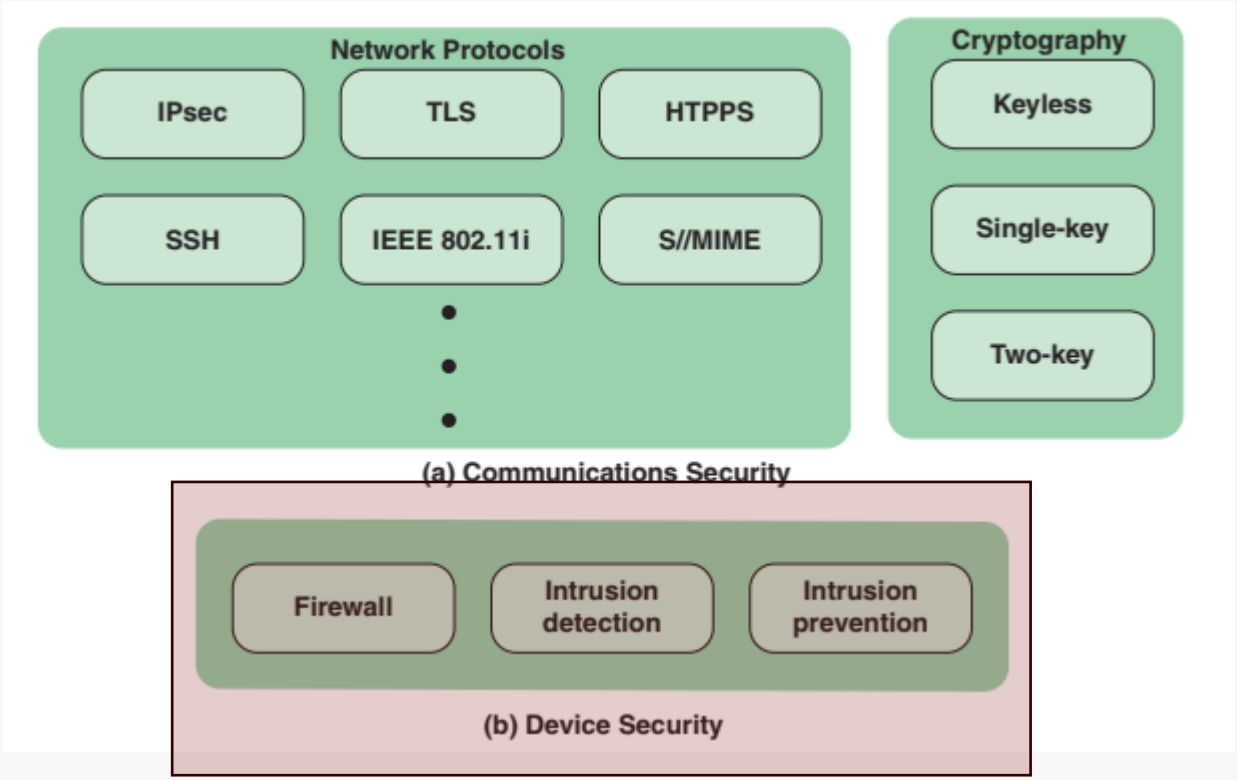


Elemen kunci pada network security

Device Security

Network security mencakup perlindungan perangkat (*device*) seperti router, switch, dan sistem klien/server dari penyusup, malware, dan beban berlebih yang dapat mengurangi availability sistem.

Deteksi Intrusi➔ perangkat keras atau lunak yang menganalisis informasi jaringan atau komputer untuk mendeteksi dan memberikan peringatan terhadap upaya akses tidak sah secara real-time.

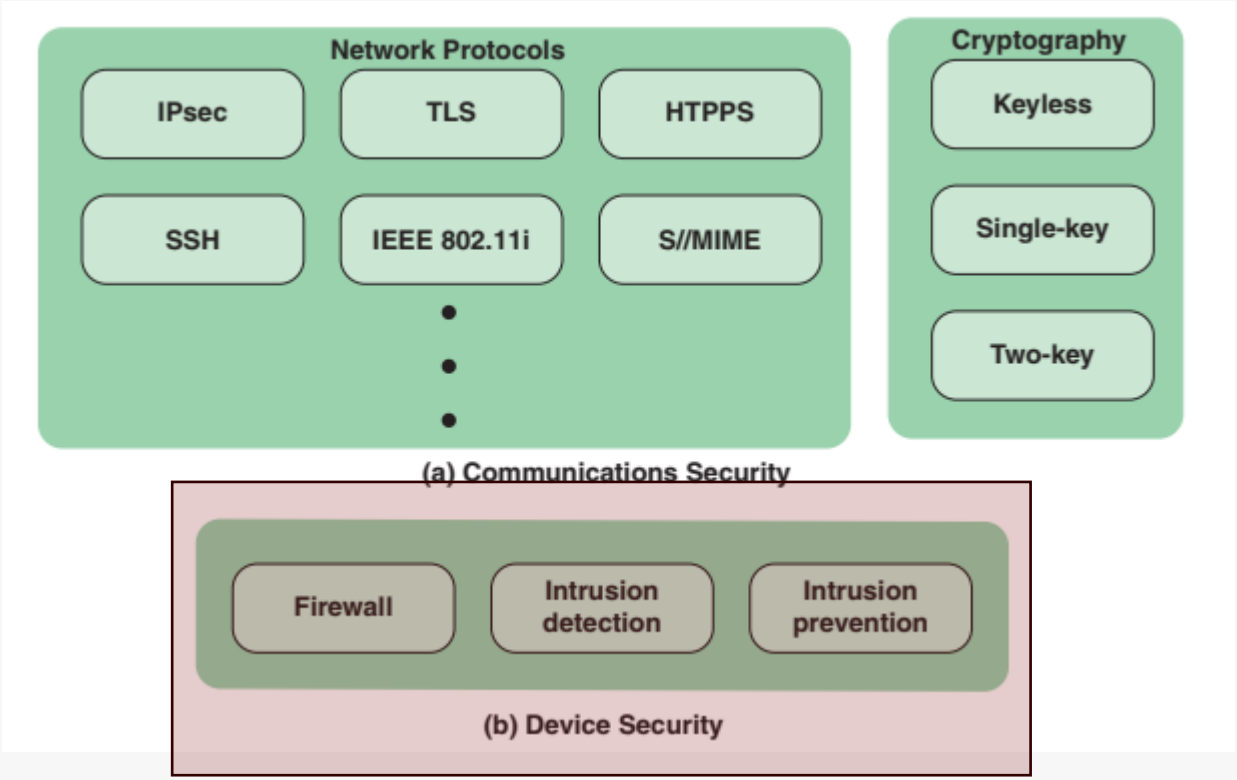


Elemen kunci pada network security

Device Security

Network security mencakup perlindungan perangkat (*device*) seperti router, switch, dan sistem klien/server dari penyusup, malware, dan beban berlebih yang dapat mengurangi availability sistem.

Pencegahan Intrusi➔ perangkat keras atau lunak yang mendeteksi dan menghentikan aktivitas intrusi sebelum mencapai target.



Elemen kunci pada network security

Information Privacy Concepts

1980s–1990s

- 1984, the UK Passes the Data Protection Act
- 1995, the Data Protection Directive is Passed in the EU

2000

European Commission Decides

- U.S. Companies Complying With a Self-Certification Program Meets EU Req.'s ("**Safe Harbor Scheme**"); and
- Allows to Transfer Data From EU to U.S. ("**Safe Harbor Decision**")

2001

- **Sept. 11** Terrorist Attack
- **Oct. 26** the U.S. Congress Passes and President Bush Signs into Law the U.S. Patriot Act Which Enables the U.S. Gov't to Obtain Stored Data From any Company Without Court Order

2004–2005

- Canada Enacts PIPEDA
- Canada's British Columbia Privacy Commissioners Begins Exams U.S. Patriot Act; Creates Requirements
- Complaints From Canadian Imperial Bank of Commerce VISA Customers re: Cardholder Agreement Saying Bank is Using U.S. Providers and Data is Subject to U.S. Patriot Act

2008–2010

- **Dec. 2008**, Chris Connelly of Galexia, an Australian Consultancy Firm, Reports Problems With Safe Harbor.
- **Feb. 25, 2010**, the European Commission Adopts Standard Contractual Clauses to/From Countries Found "inadequate".

2011

- **April–June 2011** Zack Whittaker Reports on Google and UK Universities, and Microsoft
- **Oct. 2011** Dutch Minster of Safety and Justice Bans U.S. Cloud Providers But EU Struggles With Whether Ban Violates EU Competition and Internal Market Rules and WTO Govt's Procurement Agmt

June 2013

- Edward Snowden Begins to Reveal U.S. Surveillance Activities to the Guardian Including Project TEMPORA (UK's GCHQ Gathering and Sharing Intel Data Via Fiber Optics
- The German Member of European Parliament Calls for Infringement Proceedings Against U.K. (Article 16 of Treaties of EU)

Oct. 6, 2013

Austrian attorney, Max Schrems, files complaints with Ireland's Data Protection Authority against Facebook alleging Irish data transfer to U.S. inadequate in light to surveillance and no ability for EU citizen to control data.

Key Privacy Terminology

Privacy:

- Hak untuk "tidak diganggu" — artinya, bebas dari pengamatan atau gangguan.
- Kemampuan untuk mengontrol informasi yang dirilis tentang diri seseorang.

- Stanford Encyclopedia of Philosophy

Key Privacy Terminology

Information Privacy:
Hak individu untuk mengontrol atau memengaruhi informasi yang berkaitan dengan mereka, bagaimana informasi itu dikumpulkan, disimpan, dan kepada siapa serta bagaimana informasi itu diungkapkan.
- ITU-T X.800 (Security Architecture for Open Systems Interconnection)

Key Privacy Terminology

Information Privacy:
membuat informasi pribadi seseorang tidak tersedia untuk pihak-pihak yang seharusnya tidak memiliki informasi tersebut
- U.S. National Research Council report
(At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues)

informasi pribadi apa saja yang tidak boleh dishare?

Key Privacy Terminology

Privasi Informasi dan PII

PII➔personally identifiable information

Informasi yang dapat digunakan untuk mengidentifikasi atau melacak identitas seseorang

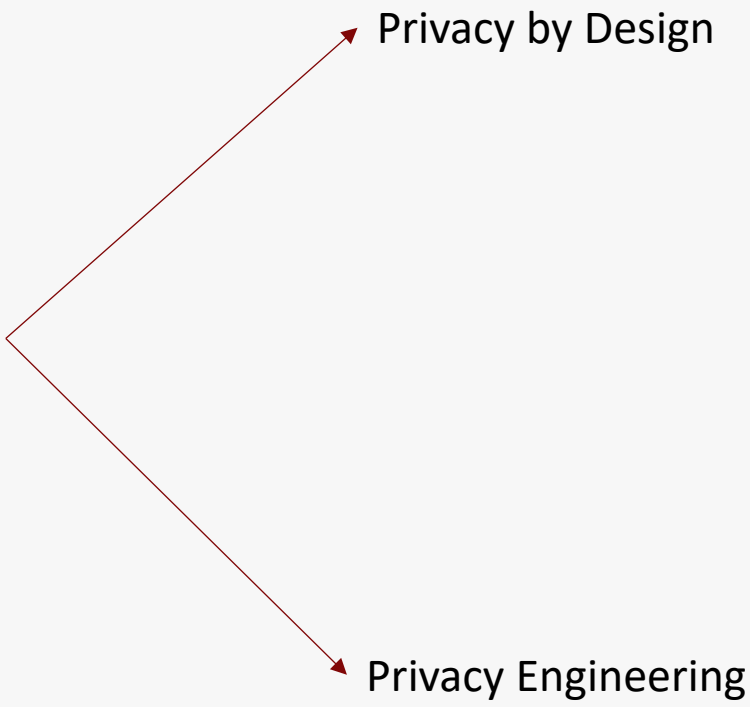

Why it is not advisable to share your ID card online.
ID
EXPLAINING WHY.COM

Key Privacy Terminology

Contoh PII menurut NIST SP 80-122 meliputi:

- Nama lengkap, nama gadis ibu, atau nama alias.
- Nomor identifikasi pribadi seperti nomor jaminan sosial, nomor paspor, atau nomor rekening.
- Informasi alamat seperti alamat rumah atau email.
- Informasi aset seperti IP Addres atau MAC Addres.
- Nomor telepon, termasuk nomor ponsel dan bisnis.
- Karakteristik pribadi seperti foto, sidik jari, atau data biometrik lainnya.
- Informasi tentang properti pribadi seperti nomor registrasi kendaraan.
- Informasi yang terkait dengan individu, seperti tempat lahir, agama, pekerjaan, pendidikan, atau informasi kesehatan.

Key Privacy Terminology

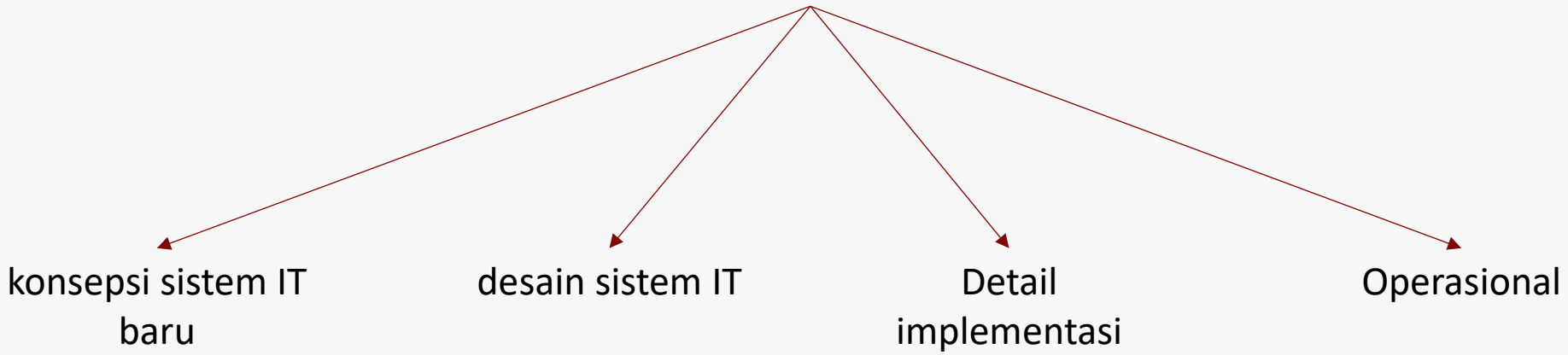


Key Privacy Terminology

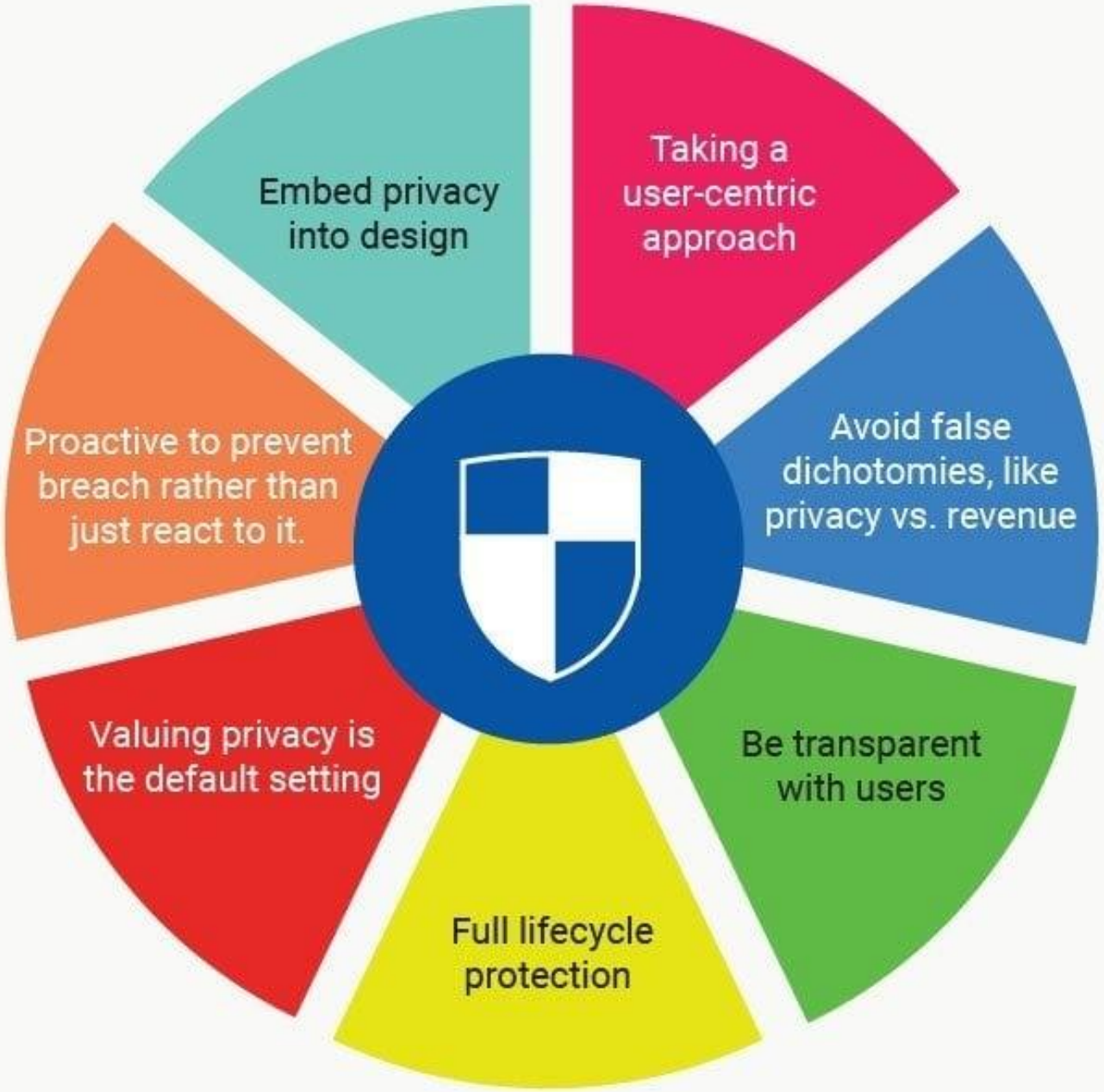
Privacy by Design

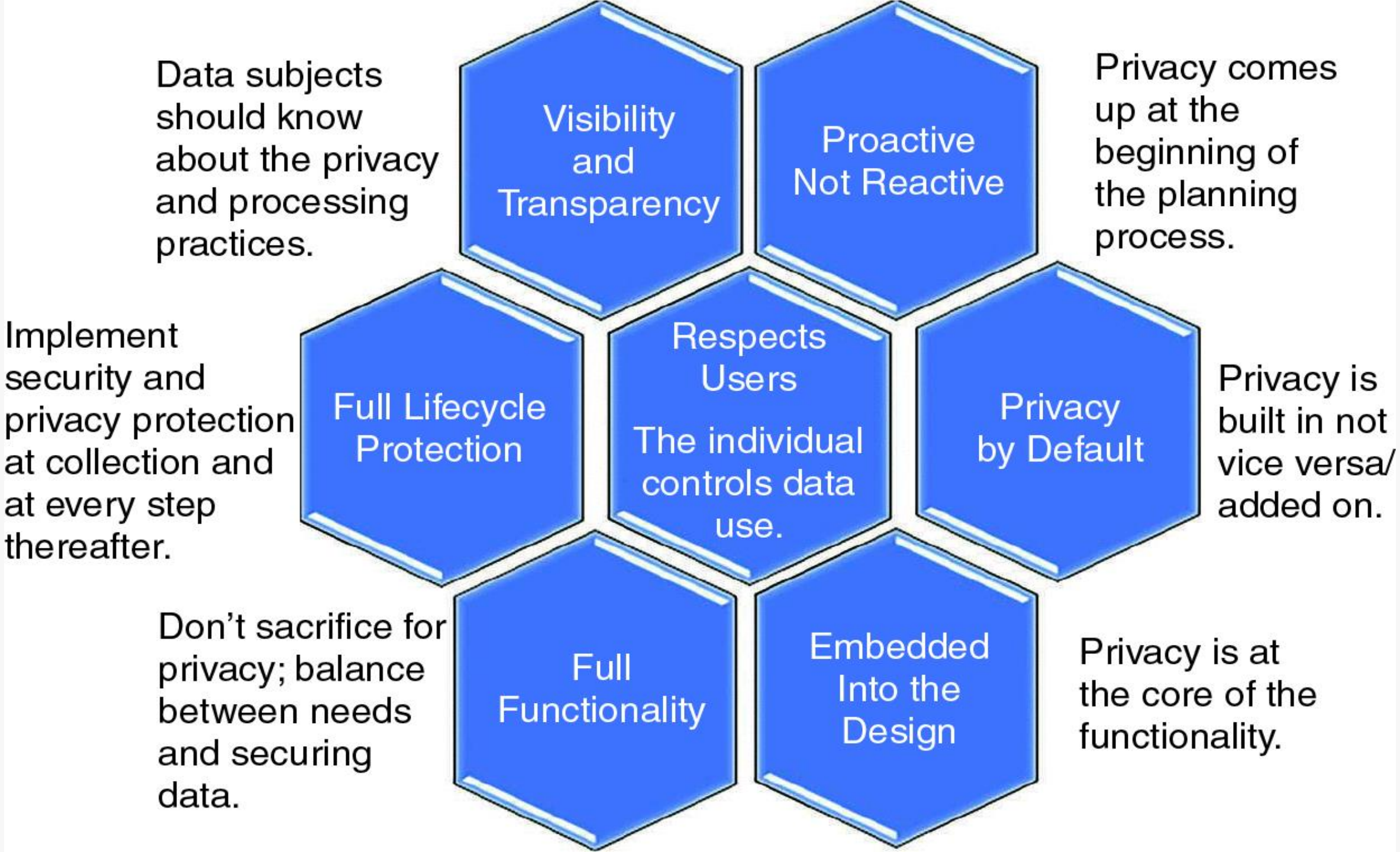
mempertimbangkan privasi sepanjang proses pengembangan sistem, mulai dari konsepsi sistem IT hingga desain sistem secara detail, implementasi, dan operasionalnya.

Praktik yang mempertimbangkan langkah-langkah perlindungan privasi sejak tahap desain sistem.
-**ISO 29100** (Information Technology—Security Techniques—Privacy Framework)



Privacy by Design




Data subjects should know about the privacy and processing practices.
Visibility and Transparency
Proactive Not Reactive
Privacy comes up at the beginning of the planning process.
Implement security and privacy protection at collection and at every step thereafter.
Full Lifecycle Protection
Respects Users
The individual controls data use.
Privacy by Default
Privacy is built in not vice versa/ added on.
Don’t sacrifice for privacy; balance between needs and securing data.
Full Functionality
Embedded Into the Design
Privacy is at the core of the functionality.

Key Privacy Terminology

Privacy Engineering

Privacy engineering is an emerging field that develops the tools, methodologies, and processes for meeting the privacy requirements and expectations of regulators and customers.
-**https://www.computer.org/csdl/magazine/co/2022/10/09903879/1H0G8Iq3qDu**

Key Privacy Terminology

Privacy Engineering

pertimbangan privasi selama siklus hidup sistem ICT (information and communications technology), sehingga privasi menjadi bagian integral dari fungsinya.

privacy engineering adalah disiplin khusus dalam *systems engineering* yang berfokus pada:
-**NISTIR 8062** (An Introduction to Privacy Engineering and Risk Management in Federal Systems)

bertujuan mengurangi risiko yang terkait dampak privasi dan memungkinkan pengambilan keputusan yang efisien tentang kontrol dan sumber daya

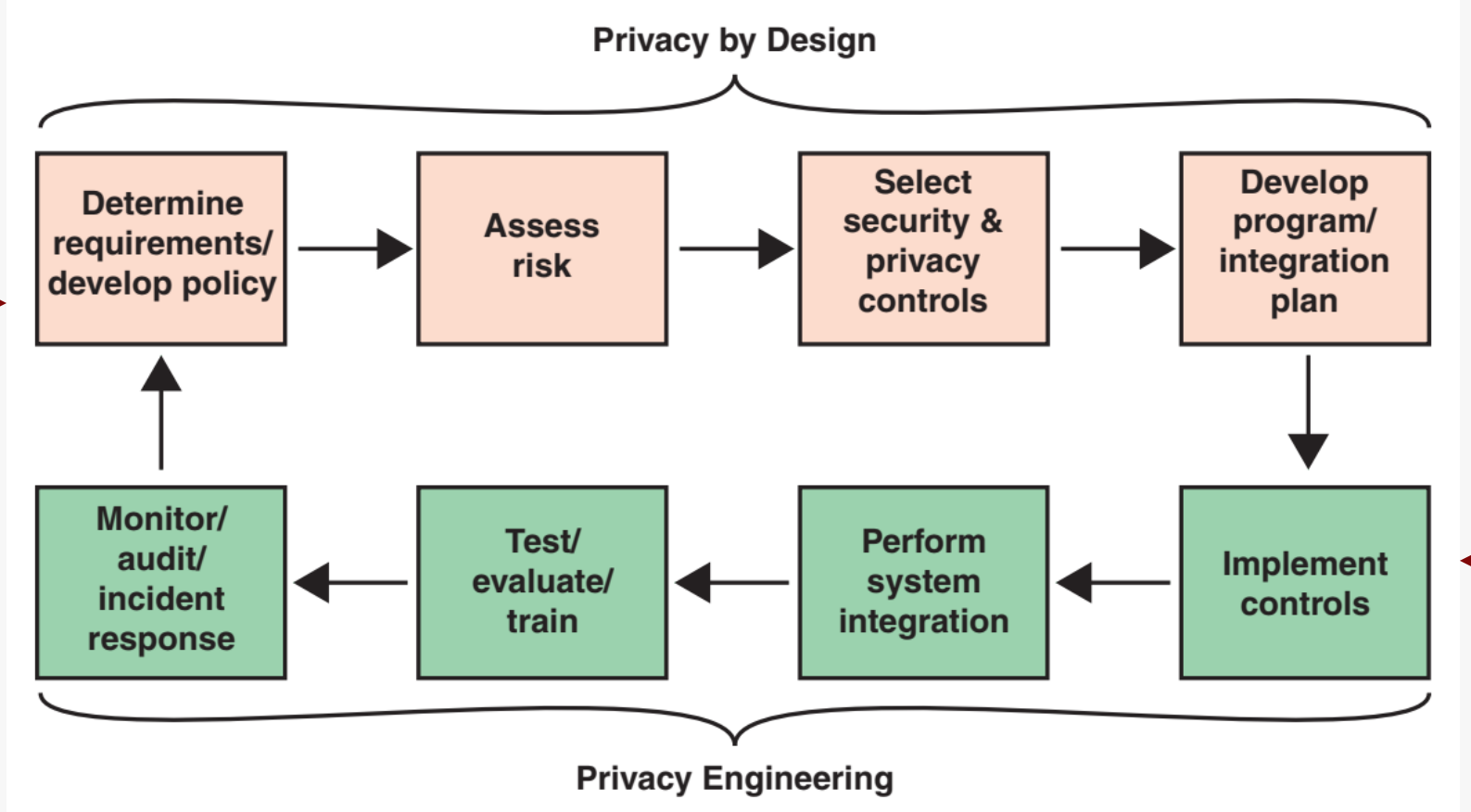
Hubungan antara Privacy by Design dan Privacy Engineering

prinsip Privacy by Design harus diterjemahkan ke dalam metodologi Privacy Engineering agar dapat diimplementasikan dengan baik.
-**European Data Protection Supervisor (EDPS)**

Hubungan antara Privacy by Design dan Privacy Engineering

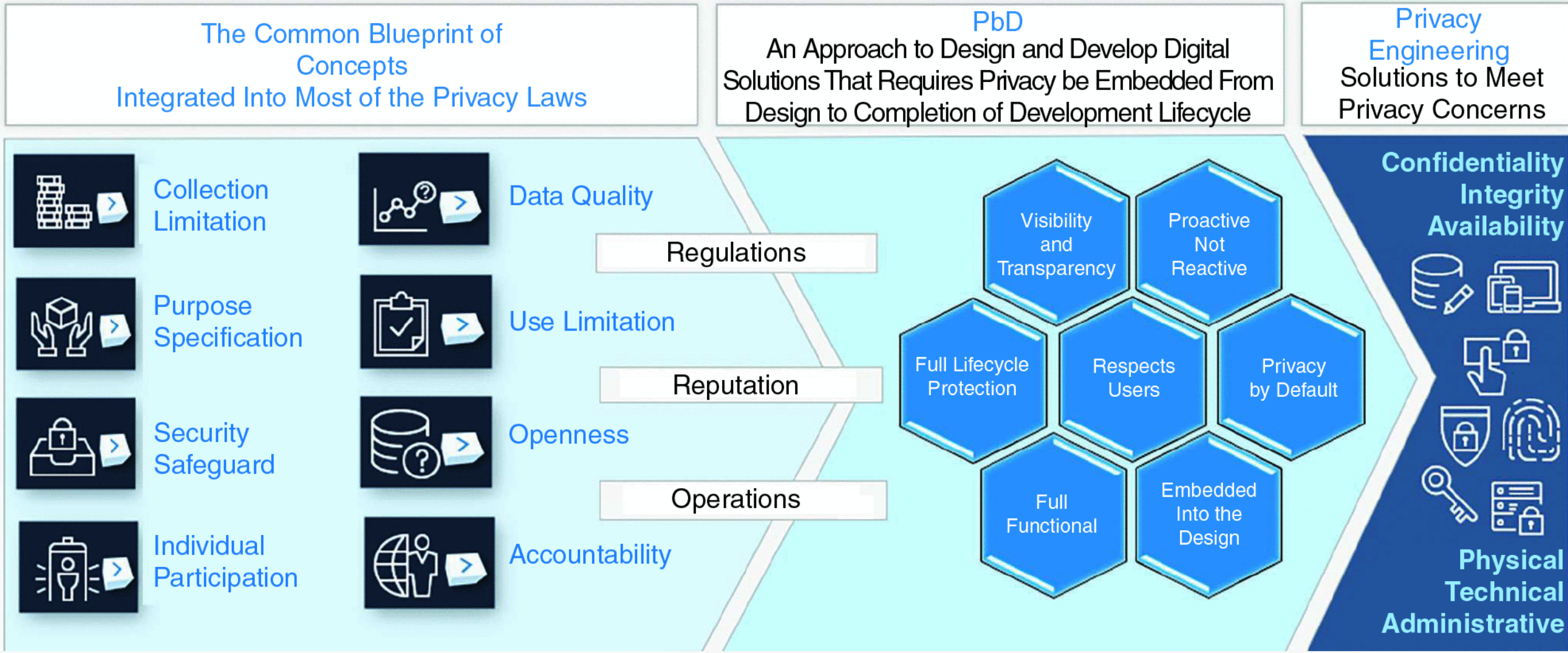
Alur mengintegrasikan perlindungan privasi ke dalam sistem informasi yang dikembangkan oleh organisasi

Fokus ke desain : menentukan kebutuhan dan cara memenuhinya



Information Privacy Development Life Cycle

implementasi dan operasional fitur privasi sebagai bagian dari sistem secara keseluruhan


The Common Blueprint of Concepts Integrated Into Most of the Privacy Laws
PbD
An Approach to Design and Develop Digital Solutions That Requires Privacy be Embedded From Design to Completion of Development Lifecycle
Privacy Engineering
Solutions to Meet Privacy Concerns
Collection Limitation
Purpose Specification
Security Safeguard
Individual Participation
Data Quality
Use Limitation
Openness
Accountability
Regulations
Reputation
Operations
Visibility and Transparency
Proactive Not Reactive
Full Lifecycle Protection
Respects Users
Privacy by Default
Full Functional
Embedded Into the Design
Confidentiality
Integrity
Availability
Physical
Technical
Administrative

CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Terima Kasih
Tuhan Memberkati