Protection of Personal and Sensitive Data in Akamai CDN and Security Services

Lukasz Orzechowski, Senior Technical PgM, Akamai InfoSec

Agenda

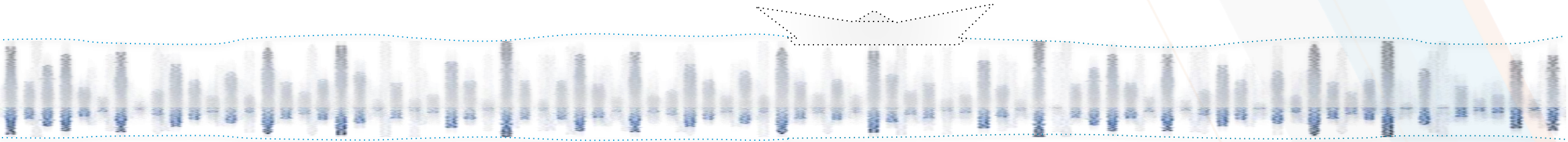**1** Introduction

2 Types of Data

3 Processing Locations
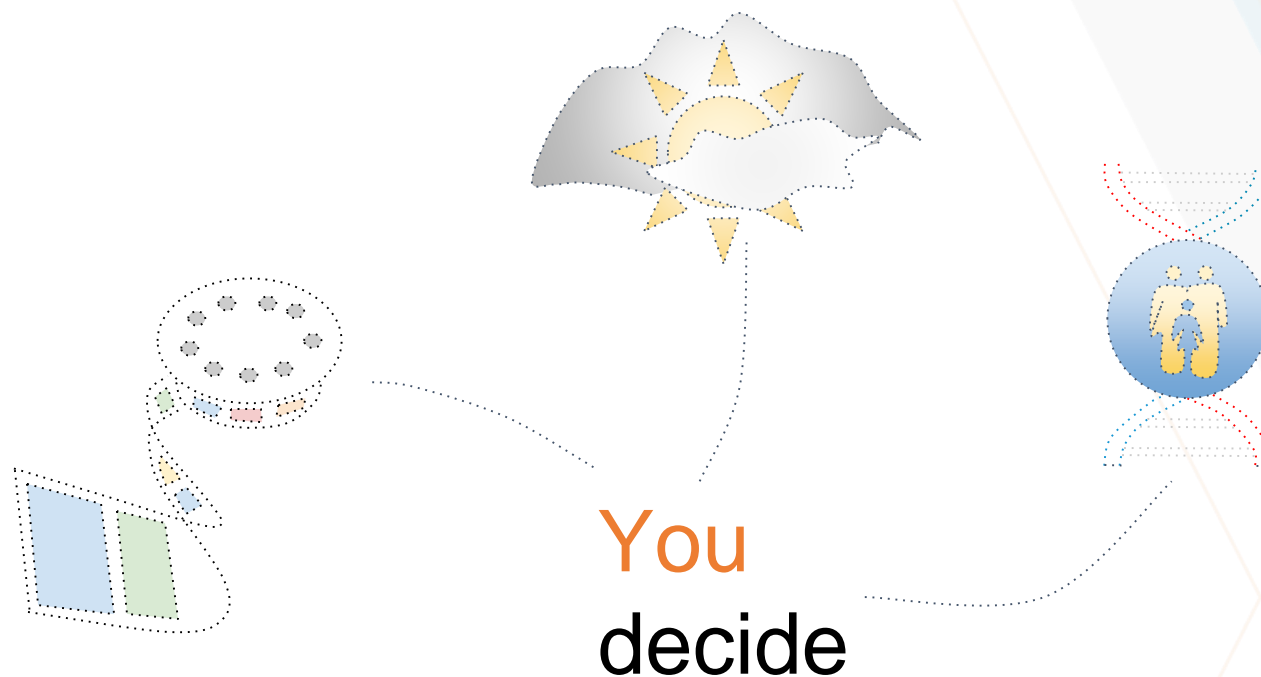
4 Access Control

5 Privacy Laws

Akamai *Experience the Edge*

How Akamai operates

Akamai acts as a conduit

Between you and your end users

You can send any type of data through Akamai

You
decide

Akamai Experience the Edge

Purpose of the presentation

This deck will help you
navigate current law landscape,
understand what data Akamai
processes and how this data
is processed & protected

Akamai *Experience the Edge*

Types of Data
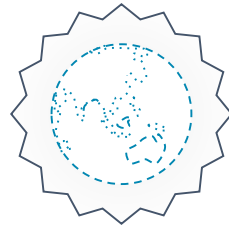
Akamai *Experience the Edge*
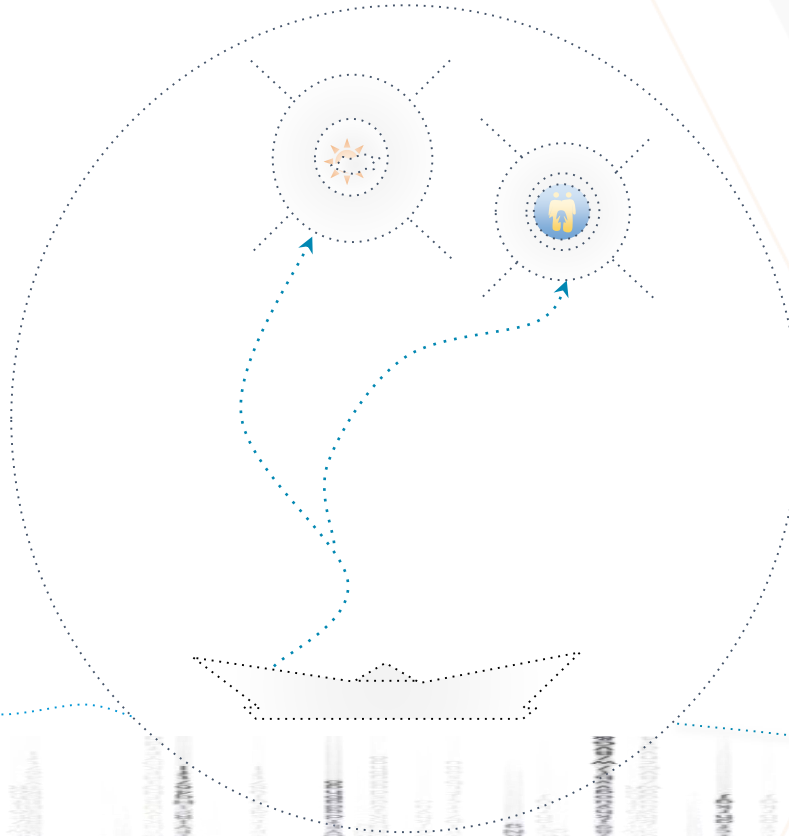
Types of Data processed by Akamai
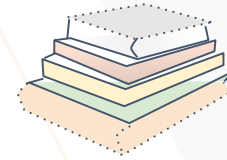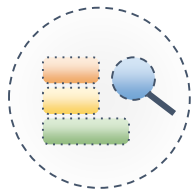
Data that flows through
Akamai platform

Data about you
as our customer

Data generated
by Akamai

Cache

Secrets

Each data category will be further discussed on the following slides

Akamai Experience the Edge

Data that flows through Akamai Platform

Akamai respects your privacy and will act as a mere conduit for data in customer content. The data will be processed exactly in the way you have configured, without inspecting it for sensitive or private information.

It can be anything

We encourage you to implement a data classification mechanism and select Akamai services adequate to the type of data you are sending.

Akamai must inspect requests to process them in the way you have ordered us to
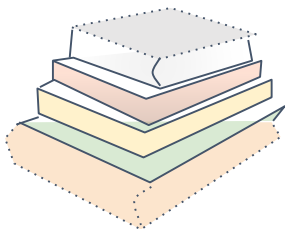
Akamai must process IP addresses

IP addresses are important as they are considered to be personal data by certain privacy laws. More about it later.

Akamai Experience the Edge

Cache

You have full control on what will be cached by Akamai

Only data selected by the customer is cached to be shared.
That's why you should not configure the services to cache sensitive or personal information (Akamai's PS team can help you with the configuration).

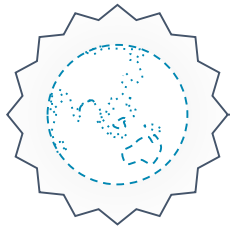Elements cached will be served by Akamai which offloads your infrastructure

Cache integrity is ensured by checksums. Cache is not encrypted at rest for performance reasons

Cache has transient nature and an expiration date. As a temporary copy, it is not backed up.

Akamai Experience the Edge

Data about you as a customer

Personal information

business address

contact names   telephone numbers

title   Luna / API credentials

email address

Regular information

services configurations   runbook rules

property information

your certificates   notification preferences

Akamai *Experience the Edge*

Data generated by Akamai

End users
IP addresses
Geo location
Page activity and URLs
Telemetry data

Bots
Bot signatures
Behavioral patterns
Bot activity
Attack patterns

Administrative
Authgate grants
Grants usage
Systems monitoring
Secret keys management
...

Internet
IP reputation
Optimal routing
Traffic congestions
Emerging threats
...

Akamai Experience the Edge

What about secrets?

Certificates and Keys

Used to encrypt connections in the Standard and Enhanced TLS CDN. Stored and distributed using Akamai Key Management Infrastructure.

Protection

Physical protection
Encryption at rest
Quarterly pentests
Encryption in transit
Dedicated memory

Port hardening
NOCC monitoring

Access control

No PII on disc
Audits every 20 minutes

Restricted inbound traffic

Akamai Experience the Edge

Processing Locations

Akamai *Experience the Edge*

Akamai is a global platform

300 000+ servers

2 300+ datacenters

130+ countries

1600+ networks

Data as of September 2017

Akamai *Experience the Edge*

Servers are close to the end users
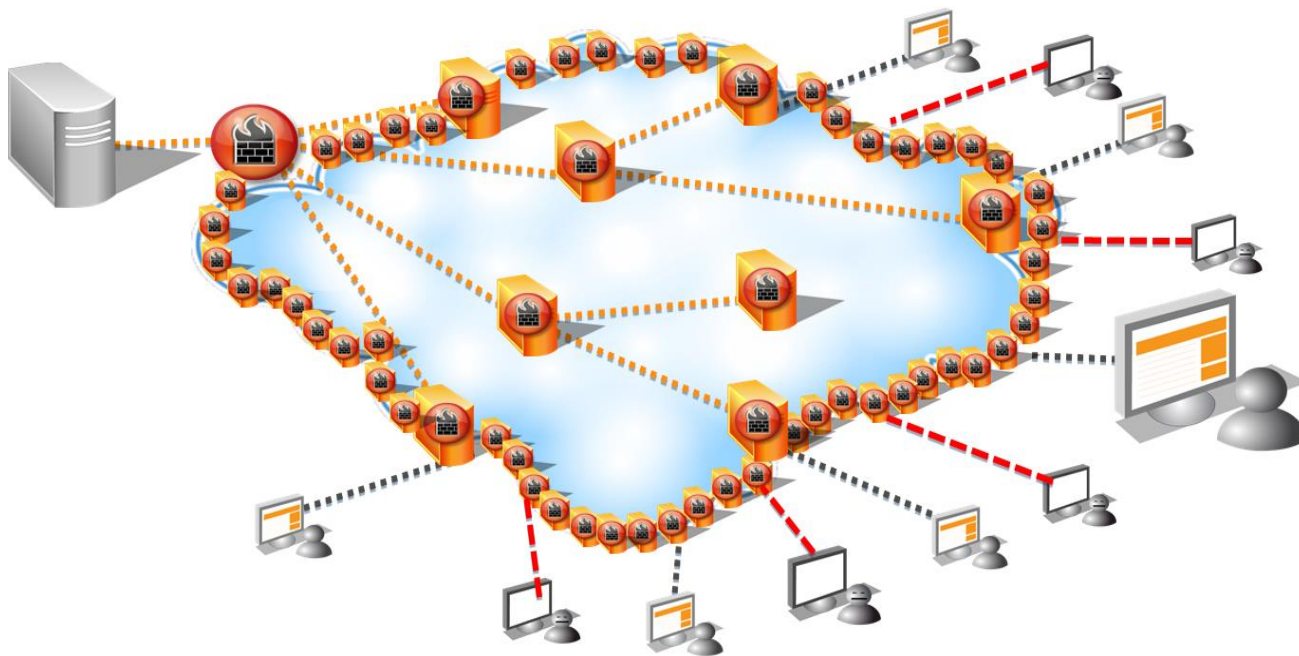
Everything is processed globally*

Data that flows through
the Akamai platform

Processed globally by the edge
servers that are the most optimal for
the end user.

Edge server inspects end user
requests and then processes them as
defined by the customer.

IP data and geolocation is used to
determine optimal servers and routing

Akamai *Experience the Edge*

Everything is processed globally*

Data that flows through the Akamai platform

Data about you as our customer

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing

Personal information is stored in Luna & Salesforce cloud and processed by Akamai support centers globally

Regular information (configuration) is distributed globally and processed by servers delivering services.

Akamai Experience the Edge

Everything is processed globally*

Data that flows through the Akamai platform

Data about you as our customer

Data generated by Akamai

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing

Personal information is stored in Luna & Salesforce cloud and processed by Akamai support centers globally

Regular information (configuration) is distributed globally and processed by servers delivering services.

Generated globally and processed globally.

Usage: services delivery, support, billing, audit trail, diagnostic, services improvement…

Akamai *Experience the Edge*

Everything is processed globally*

Data that flows through the Akamai platform

Data about you as our customer

Data generated by Akamai

Cache

Secrets

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing

Personal information is stored in Luna & Salesforce cloud and processed by Akamai support centers globally

Regular information (configuration) is distributed globally and processed by servers delivering services.
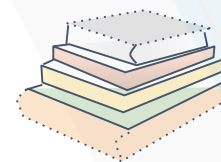
Generated globally and processed globally.

Usage: services delivery, support, billing, audit trail, diagnostic, services improvement…
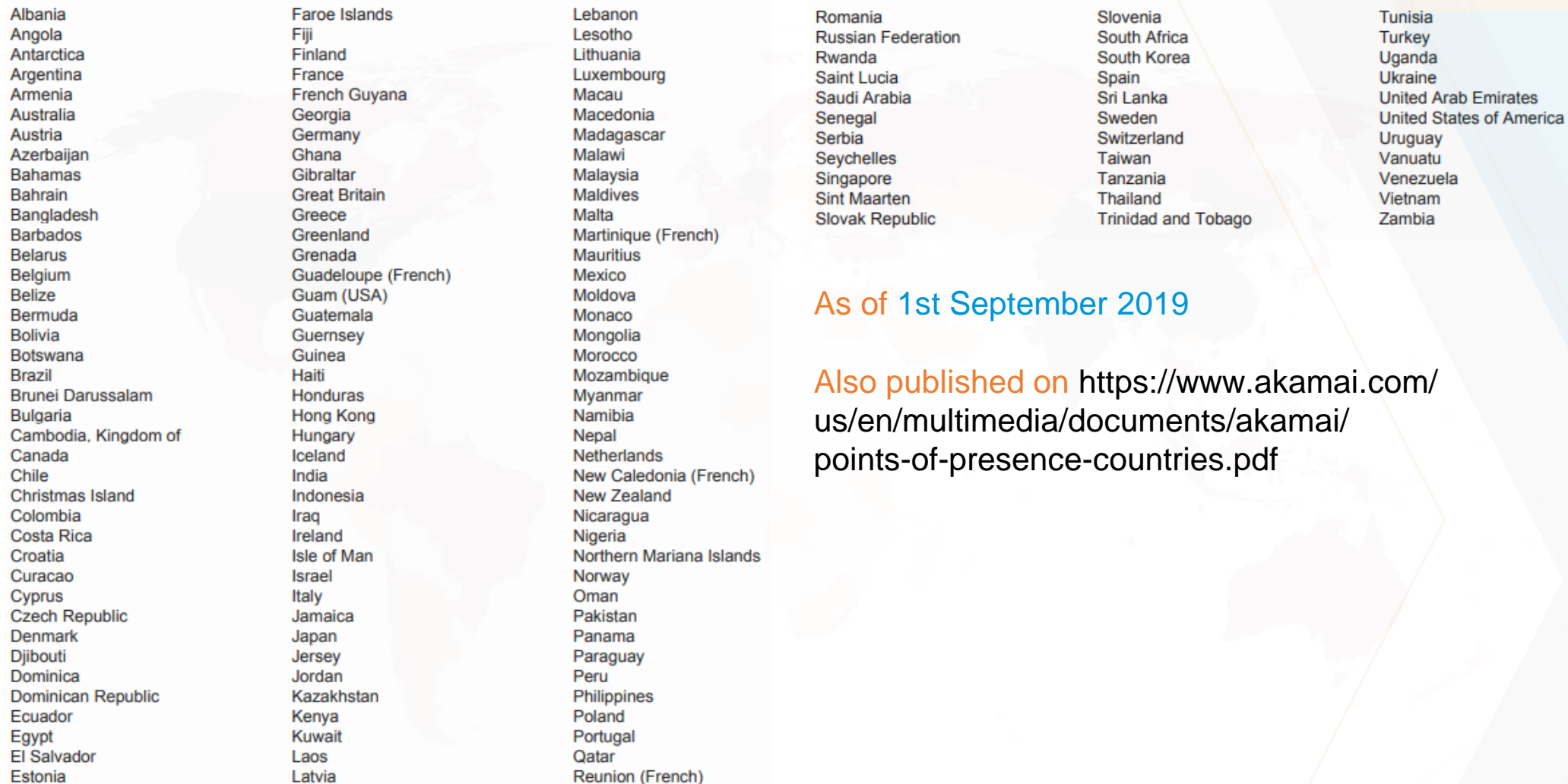
Processed and stored globally.

Managed globally by secure Key Management Infrastructure.

Processed globally by Secure CDN Edge servers

(Akamai) Experience the Edge

Can you deliver us a list of countries?

Albania
Angola
Antarctica
Argentina
Armenia
Australia
Austria
Azerbaijan
Bahamas
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Belize
Bermuda
Bolivia
Botswana
Brazil
Brunei Darussalam
Bulgaria
Cambodia, Kingdom of
Canada
Chile
Christmas Island
Colombia
Costa Rica
Croatia
Curacao
Cyprus
Czech Republic
Denmark
Djibouti
Dominica
Dominican Republic
Ecuador
Egypt
El Salvador
Estonia

Faroe Islands
Fiji
Finland
France
French Guyana
Georgia
Germany
Ghana
Gibraltar
Great Britain
Greece
Greenland
Grenada
Guadeloupe (French)
Guam (USA)
Guatemala
Guernsey
Guinea
Haiti
Honduras
Hong Kong
Hungary
Iceland
India
Indonesia
Iraq
Ireland
Isle of Man
Israel
Italy
Jamaica
Japan
Jersey
Jordan
Kazakhstan
Kenya
Kuwait
Laos
Latvia

Lebanon
Lesotho
Lithuania
Luxembourg
Macau
Macedonia
Madagascar
Malawi
Malaysia
Maldives
Malta
Martinique (French)
Mauritius
Mexico
Moldova
Monaco
Mongolia
Morocco
Mozambique
Myanmar
Namibia
Nepal
Netherlands
New Caledonia (French)
New Zealand
Nicaragua
Nigeria
Northern Mariana Islands
Norway
Oman
Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Reunion (French)

Romania
Russian Federation
Rwanda
Saint Lucia
Saudi Arabia
Senegal
Serbia
Seychelles
Singapore
Sint Maarten
Slovak Republic

Slovenia
South Africa
South Korea
Spain
Sri Lanka
Sweden
Switzerland
Taiwan
Tanzania
Thailand
Trinidad and Tobago

Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
United States of America
Uruguay
Vanuatu
Venezuela
Vietnam
Zambia

As of 1st September 2019

Also published on https://www.akamai.com/us/en/multimedia/documents/akamai/points-of-presence-countries.pdf
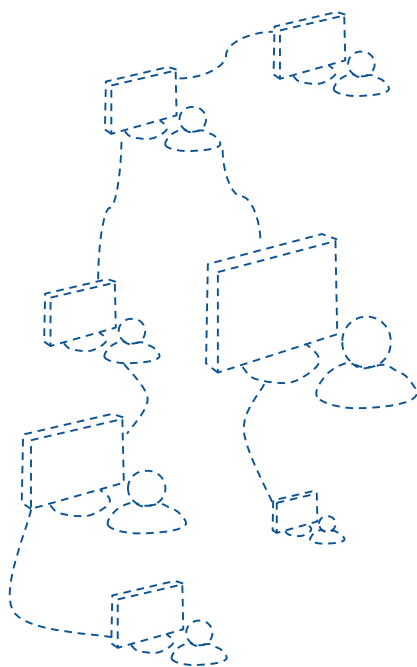
* Please note that China and Russia CDNs are offered as separate products and servers in these countries are not used in the regular CDN

Akamai *Experience the Edge*
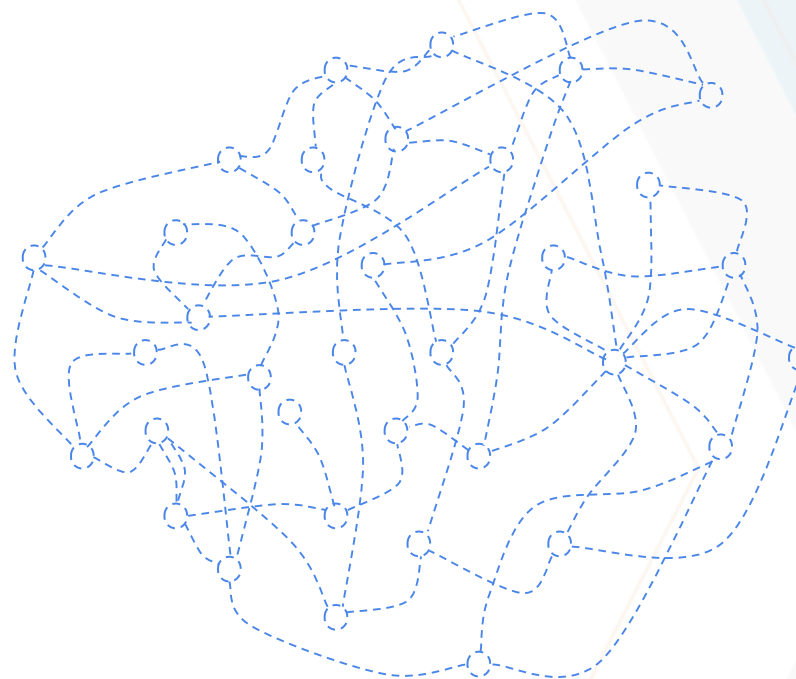
Access Control

Akamai *Experience the Edge*

Akamai networks separation

Corporate Network

Authgate

Production Network

Akamai Experience the Edge

Akamai networks separation

Corporate Network

Production Network

Authgate

Akamai Employee Grants

Time
Access
Purpose

Akamai Experience the Edge

Akamai networks separation

Corporate Network

Production Network

Authgate

Akamai
Employee
Grants

Time
Access
Purpose

Proxy
Logs

Grant
reviews

Akamai Experience the Edge

Authserver
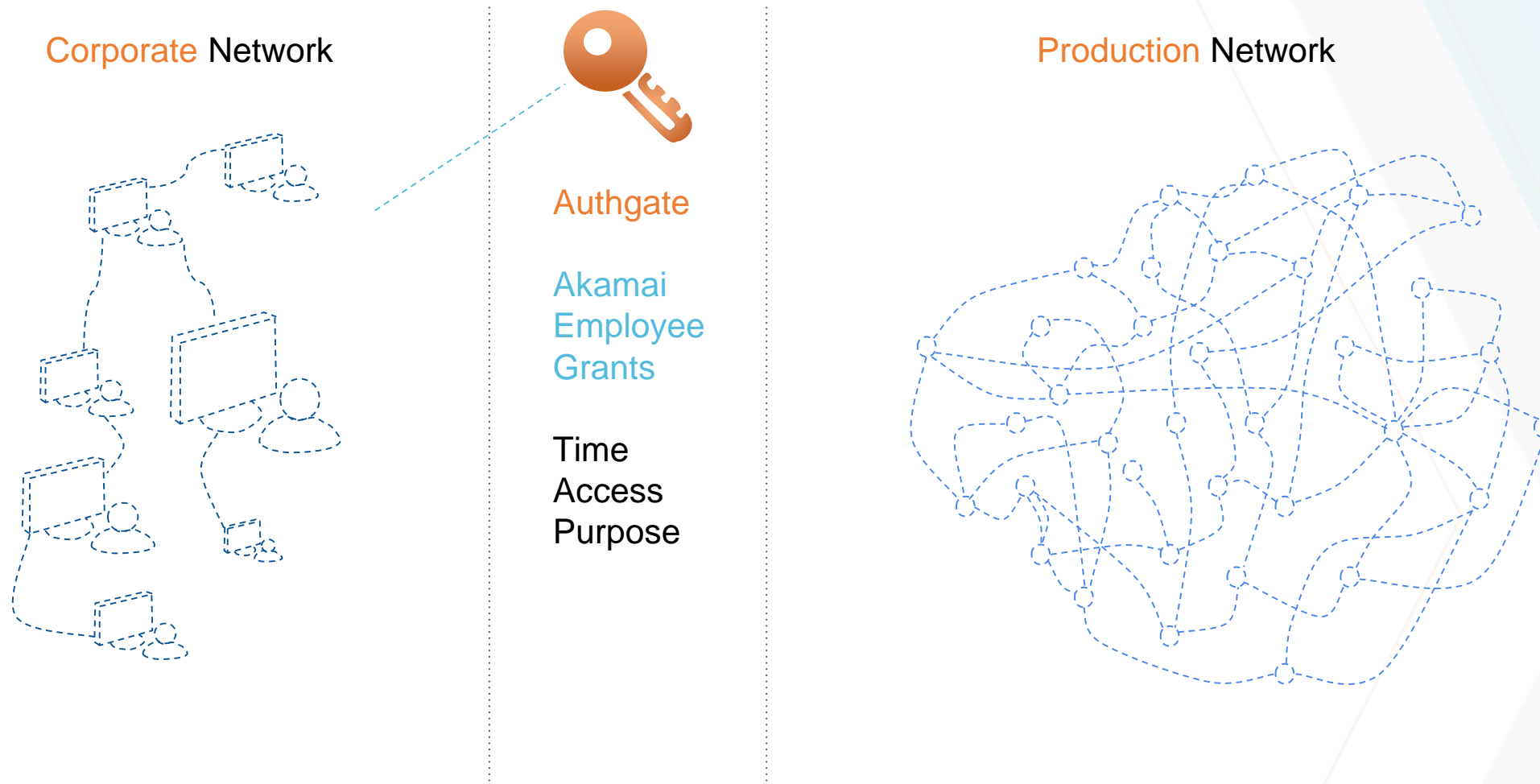
Grants users indirect access
to production machines
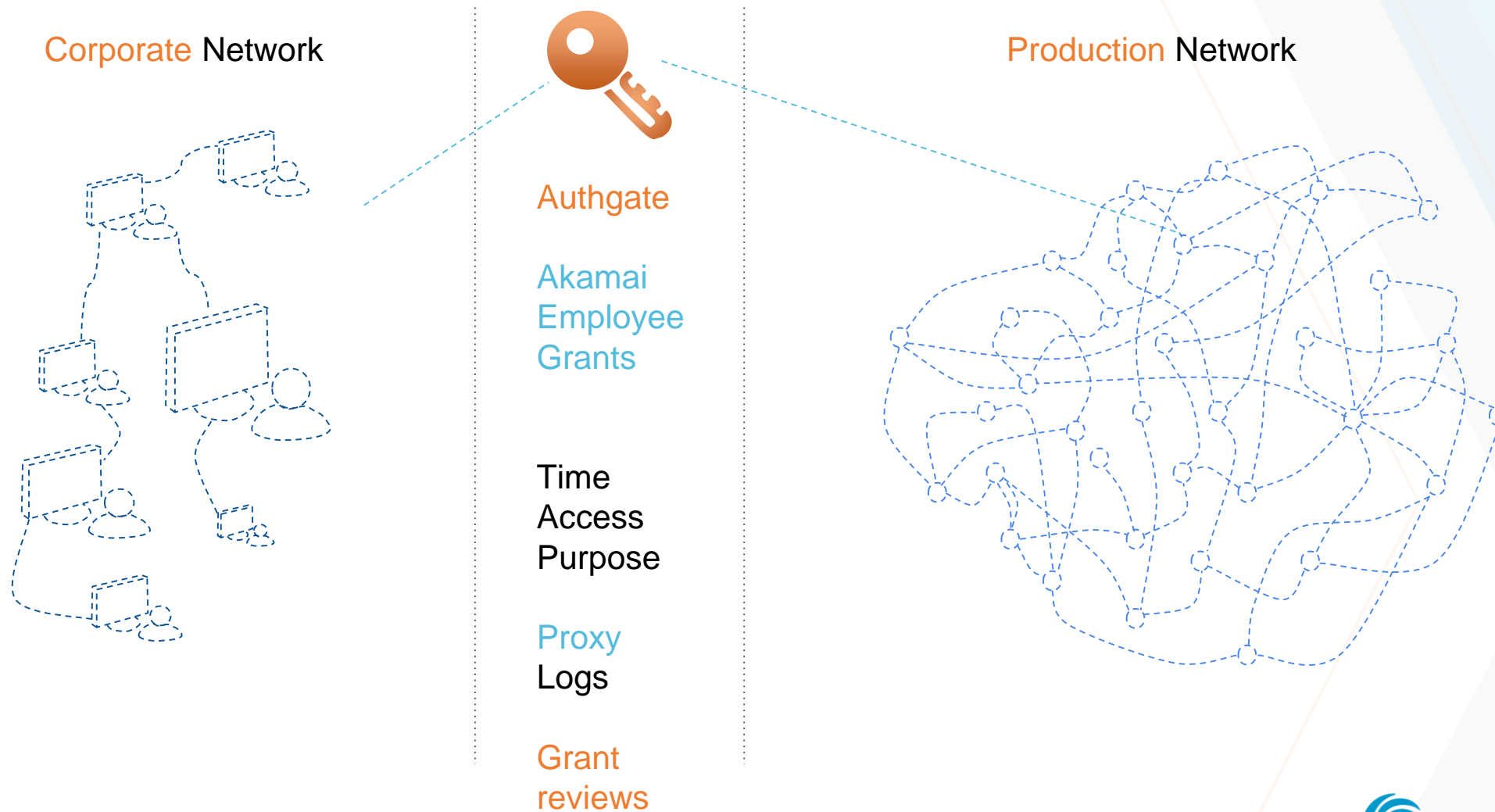
Authenticates users
using 2048 bit RSA key

Sends shell commands
to Authgate gateway

Supports MFA

Grants are time limited and
provided on a must-basis

Delivers UI
to manage grants and keys

There are no
direct administrators

Generates and stores logs

Akamai Experience the Edge

KMI and Secrets

Private key

TLS Certificate Bundle

AES-256 Encryption

Separate encrypted transfer of decryption key

Audit Server

Key Distribution Center

Secure Edge Server

Akamai Experience the Edge
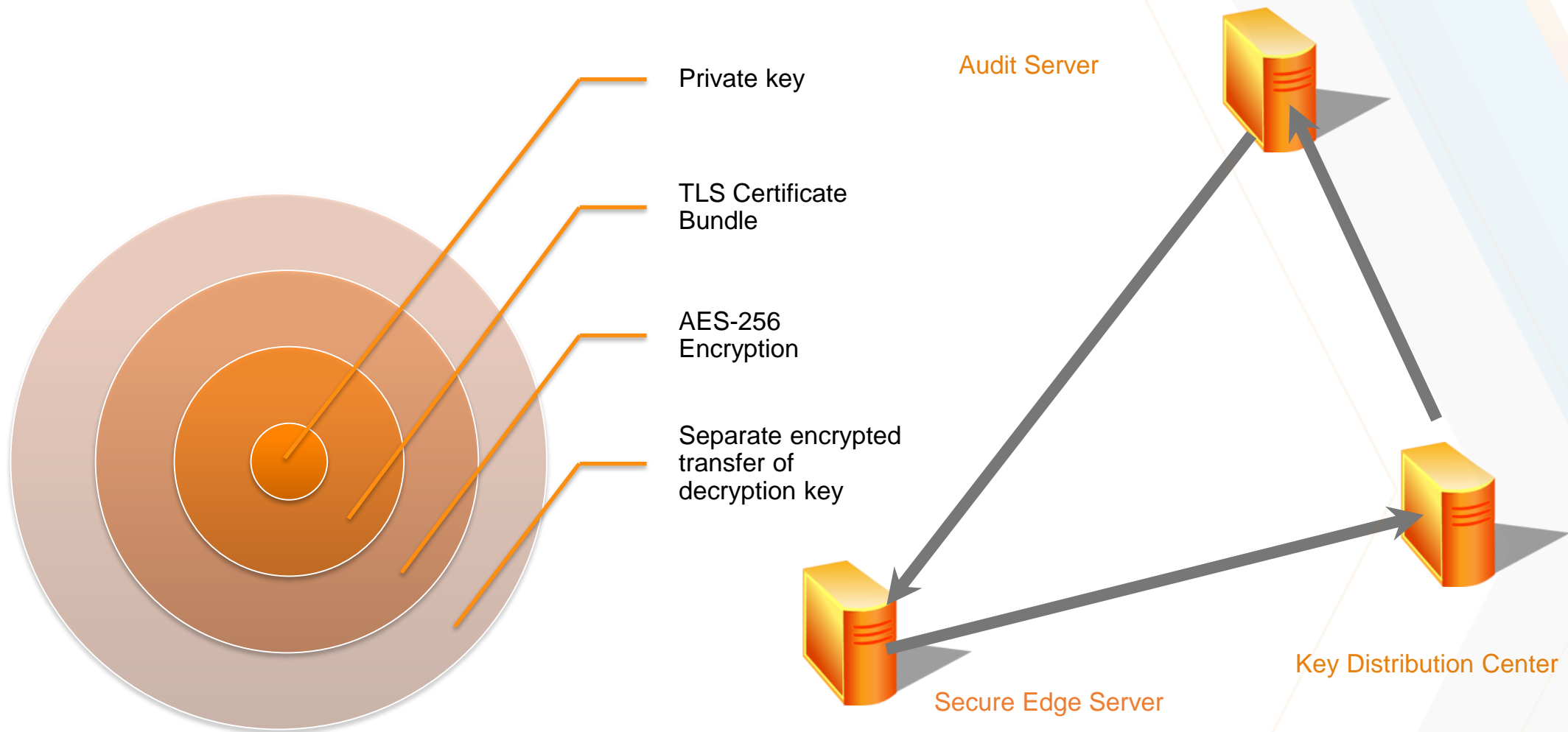
Hardened servers

Inbound traffic
only on 443 and 80

Port hardened

No PII
on disk

Secure Memory
allocation

Drop malformed
requests

Dynamic
load balancing

Dedicated
admin channels

Fully enclosed
secure racks

Multi-Layered
secret protection

Akamai Experience the Edge

Privacy Laws

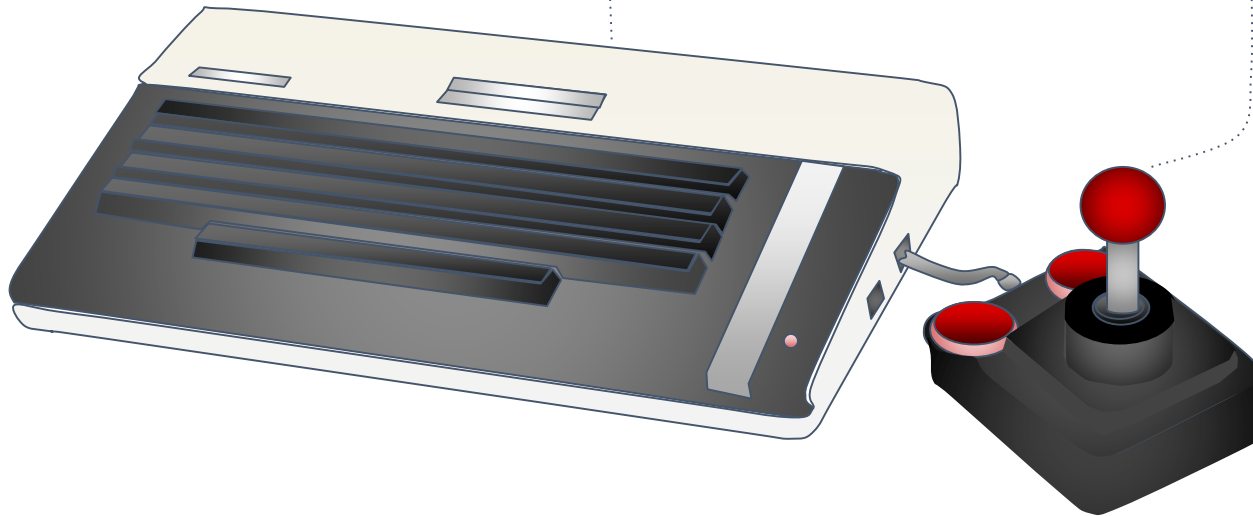| Data Protection | © 2020 Akamai | AKAMAI PUBLIC DOCUMENT

Akamai *Experience the Edge*

Privacy laws define the processing roles

The party that processes Personal Data on behalf of the determining party

The party who determines how the Personal Data is processed

The roles' name vary by country: Data Processor/Controller, Service Provider/Business, Data Intermediare/Organisation…

Akamai Experience the Edge

Akamai processing on behalf of the customer

For some Personal Data,
Akamai is processing on behalf of you as the Akamai customer
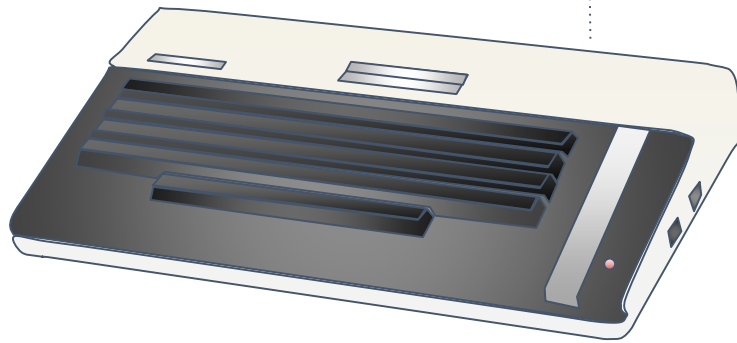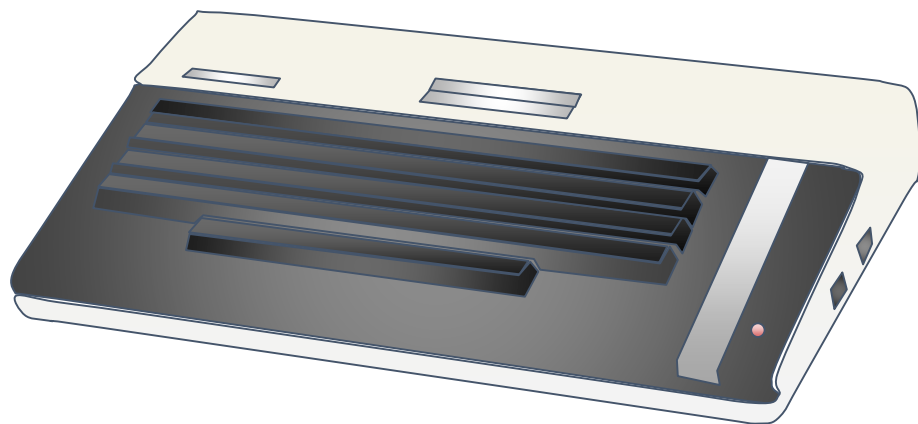
You decide what will be cached
You decide what you will send
You decide what services will be used
and therefore how the data will be processed

Data that flows through Akamai platform

Experience the Edge

Akamai processing on behalf of the customer

"Personal Data in Customer Content"

Financial or other transaction information

Subscriber name and contact information
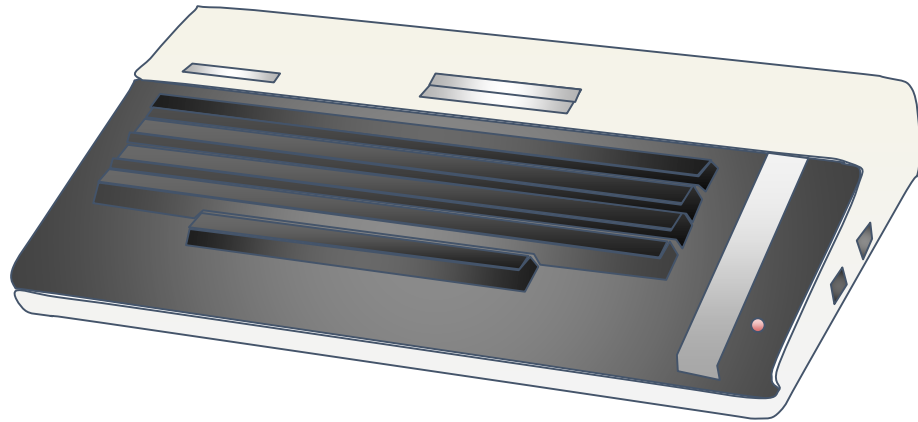
Login Credentials

Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.

Akamai processes Personal Data exactly as you have told us to process it

Akamai Experience the Edge

Akamai processing on behalf of the customer

"Personal Data in Customer Content"

Financial or other transaction information

Subscriber name and contact information

Login Credentials

Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.

You decide

You as Akamai's customer decides how the data is processed and what will be sent through the Akamai platform and, as such, you are responsible for compliance with applicable laws for such processing
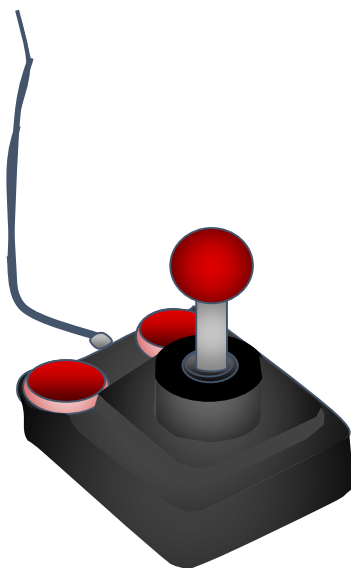
(e.g. appropriate end user notices or consent and having chosen services appropriate for the type of End User Personal Data transiting Akamai's servers.)

Akamai processes Personal Data exactly as you have told us to process it

Akamai Experience the Edge
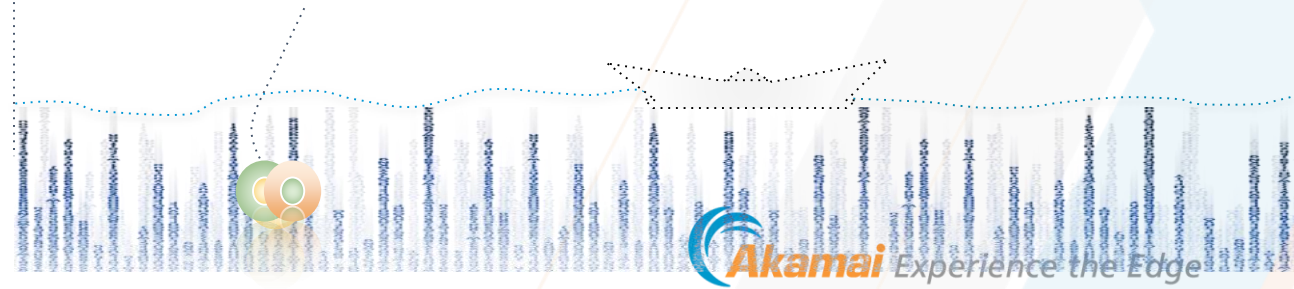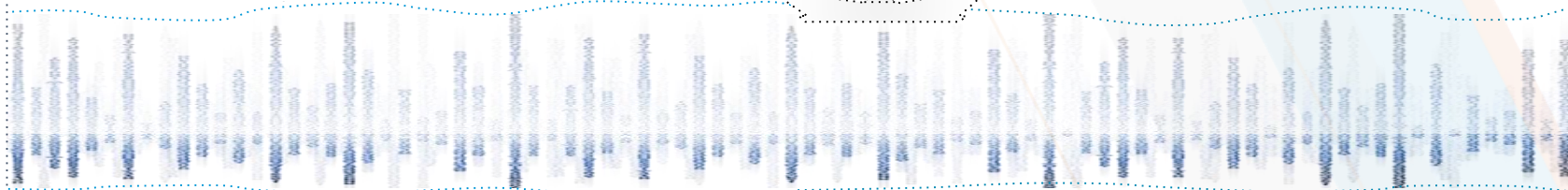
Akamai determining the purpose

"**Logged** Personal Data"

For some Personal Data,
Akamai is a Data Controller

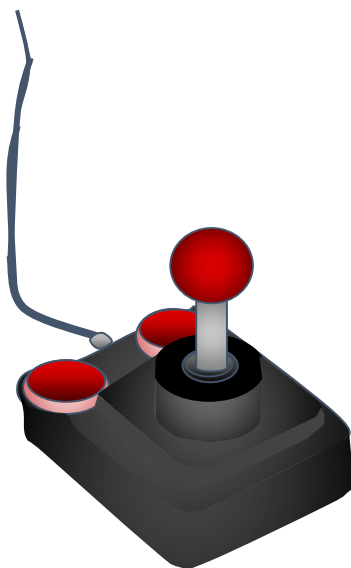Various logged data
generated by Akamai

IP addresses
Geo location
Page activity and URLs
Telemetry data

Data about you as our customer

Akamai Experience the Edge

Akamai as a Data Controller

"Logged Personal Data"

For some Personal Data, Akamai is a Data Controller

Various logged data generated by Akamai

IP addresses
Geo location
Page activity and URLs
Telemetry data

Akamai determines the data that must be collected and processed, the purposes of that processing (such as, for example, mapping/routing, threat analysis, service improvement and development, fraud management, billing), and the technical means for conducting the processing (such as development of algorithms, and delivery techniques and systems).

Experience the Edge

Akamai as a Data Controller

"Customer Personal Data"
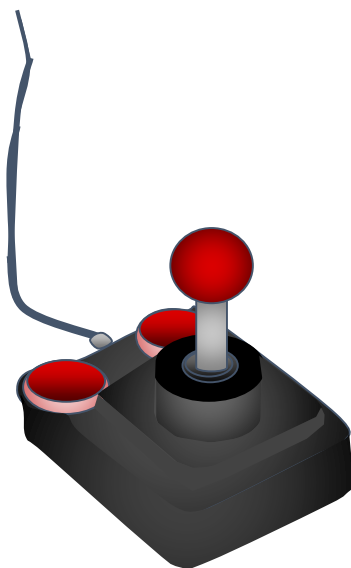
corporate address   Job title

contact names   Business phone numbers

ACC / API credentials

business email address

Data about you as our customer

Akamai collects and processes Customer Personal Data to provide access to and use of services, communications with customers, and to manage customer relations. This data is stored by Akamai in its portal(s) (such as Luna), customer community and developer sites, and in internal business process tools.

Akamai determines what data it collects from its customers (e.g. business address of the company), the data retention and the purposes such data is used for (Marketing and Relationship Management). Therefore, with respect to Customer Personal Data, Akamai operates as Data Controller.

Akamai *Experience the Edge*

Privacy Laws require a DPA

DPA sets forth the
right and duties
associated
with a processing role
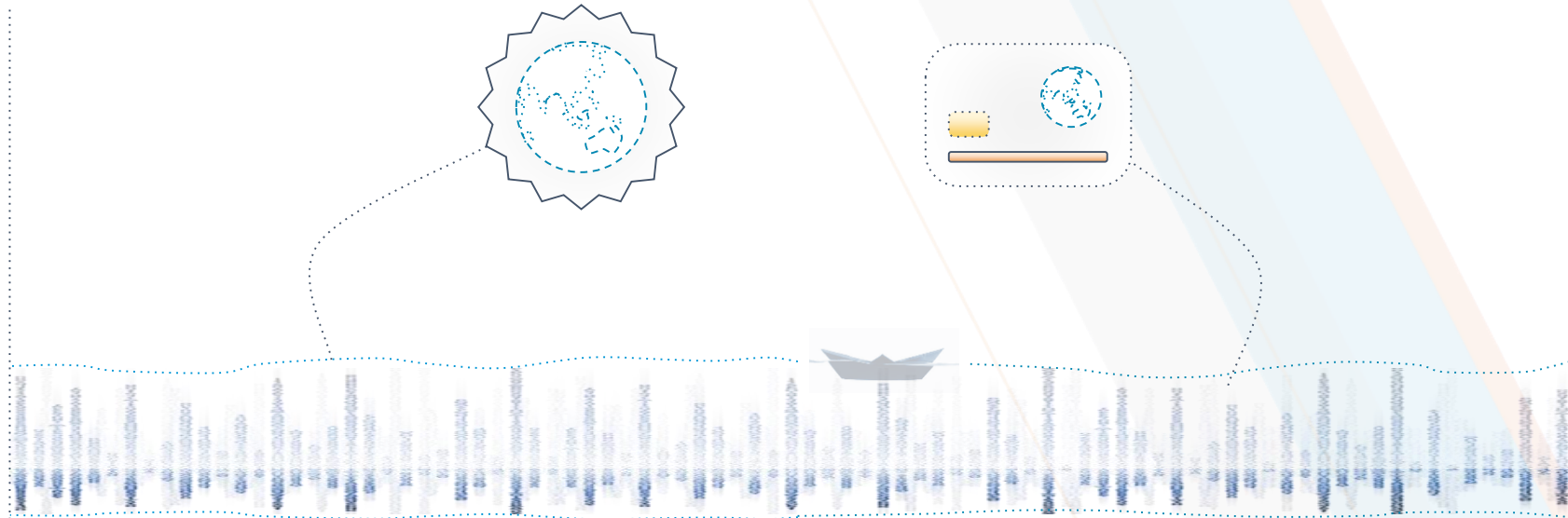
Akamai's processing activities required for providing the service is reflected in the Akamai DPA available at

https://www.akamai.com/us/en/multimedia/documents/akamai/akamai-data-protection-addendum.pdf

The Akamai DPA cover the role of Akamai as a content delivery and security service provider. Customer's DPAs require extensive work to adjust them to the Akamai services.

Akamai *Experience the Edge*

Summary

1 Introduction

2 Types of Data

3 Processing Locations

4 Access Control

5 Privacy Laws

Akamai *Experience the Edge*

Thank You

| Data Protection | © 2020 Akamai | AKAMAI PUBLIC DOCUMENT

Akamai Experience the Edge