



MCS

Gatekeeper

Exposing MCS services over the Internet

How Gatekeeper will do this

- How it works
- On-boarding process
- What it can mean for clients
- What it can mean for service providers
- Next steps

Practical demonstration

Questions and answers



Overview of MCS

- MCS has 100+ services exposed via:
 - HTTP endpoints
 - JMS over MQ
- Majority of services return customer information using an identifier
 - Party ID, billing account ID, billing account number
- Problems:
 - Identifying which clients are calling which services
 - Only accessible within Sky networks

To help solve these problems we created Gatekeeper

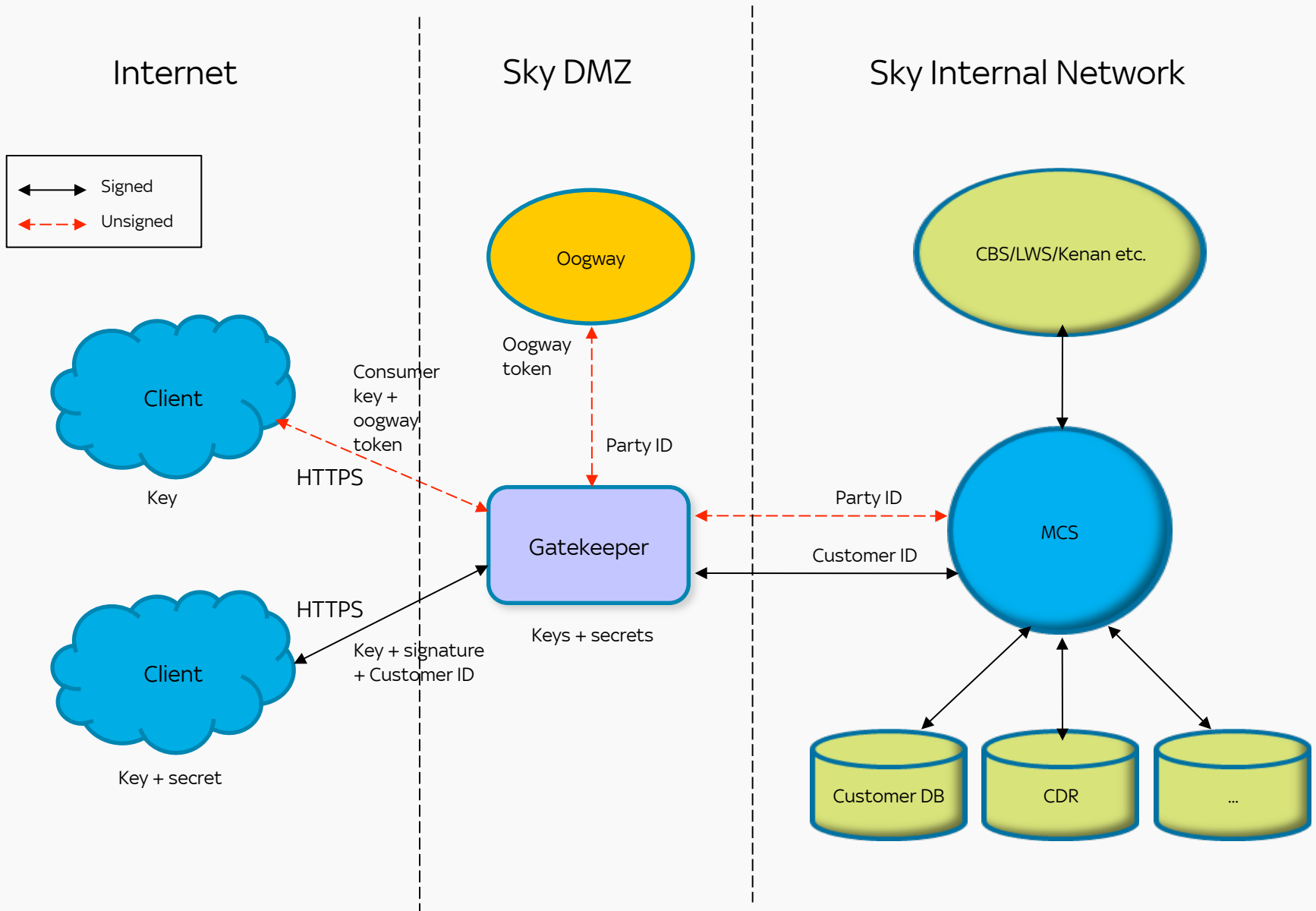


Gatekeeper

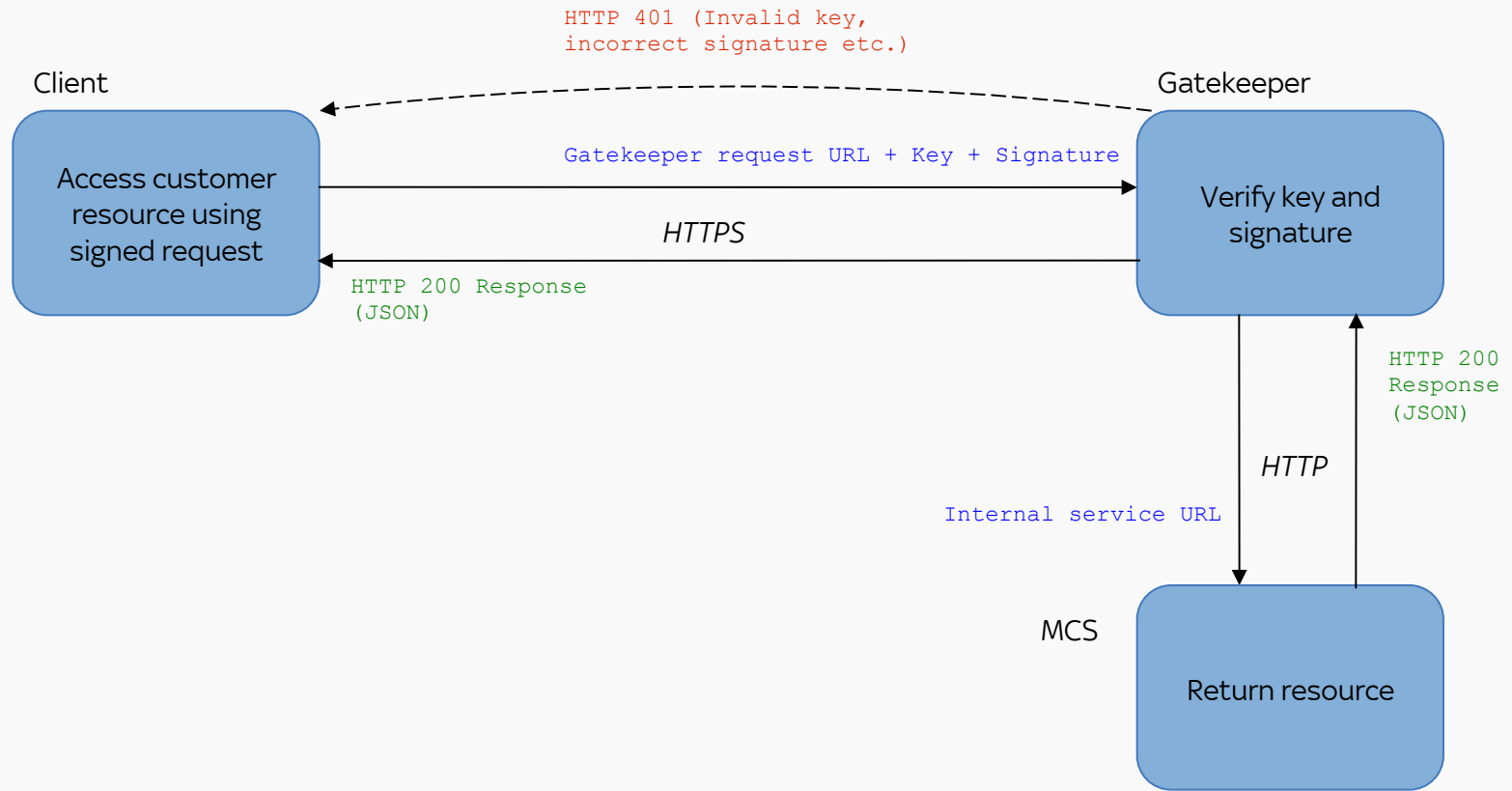
- Gatekeeper is an internet-facing HTTP service proxy:
 - Clients signed up to Gatekeeper can call MCS services within Sky securely over the internet
 - Access to individual services
 - Access granted on case-by-case basis
 - Security via OAuth 1.0a
 - Requests signed using client key and secret
 - Can access customer information using Oogway SSO token
 - Token translated to party ID by Oogway
 - HTTPS-to-HTTP



Gatekeeper Overview



Calling Gatekeeper



Client Management

- Access to services managed through separate admin app
 - Map external Gatekeeper endpoints to internal MCS service URLs
 - Grant access to individual services to clients
 - Revoke access too
 - Set service usage quota for throttling
 - Audit trail for changes
 - Who, what, when

The screenshot displays the 'Client Management Application' interface. At the top, the user is logged in as 'User: Krishan Lakha' with a 'Logout' link. On the left, there is a navigation sidebar with options: 'Publish!', '16:51:21 : Configuration has not been published yet', 'Navigation', 'Hosts & Endpoints', 'Services' (selected), 'Consumers', 'Audit', and 'DeploymentInfo'. The main area is titled 'Services' and contains a '+ Add Service' button. Below this is a table listing various services with their reference names, methods, backend hosts, and URL formats.

Reference Name	Method	Backend Host	URL Format
oogway-profile	GET	http://e05wap.oogway.bskyb.com:80/profiles	/token/{sso}
management-properties	GET	http://stage.raas.mcs.nimbus-stage.cg.sky.com:80/	management/properties
profile	GET	http://stage-mcs-identity.cg.bskyb.com:80/mcs-identity	profile/{partyIdentifier}
extendedLoginProfile	GET	http://e05-identity.mcs.bskyb.com:80/mcs-identity	extendedloginprofile/{tokenToPartyIdentifier}
entitlements	GET	http://stage-mcs-identity.cg.bskyb.com:80/mcs-identity	entitlements/{partyIdentifier}
extendedLoginProfile-e04	GET	http://e04-identity.mcs.bskyb.com:80/mcs-identity	extendedloginprofile/{tokenToPartyIdentifier}
management-vcapapplication	GET	http://stage.raas.mcs.nimbus-stage.cg.sky.com:80/	management/vcapapplication
ping-id-offline	GET	http://stage-mcs-identity-offline.cg.bskyb.com:80/mcs-identity	ping/{delay}
getContact	GET	http://stage-mcs-identity.cg.bskyb.com:80/mcs-identity	contact/{id}
Customeroverviewtest2	GET	http://stage-mcs-identity.cg.bskyb.com:80/mcs-identity	customeroverview/pid-{tokenToPartyIdentifier}
health	GET	http://stage.raas.mcs.nimbus-stage.cg.sky.com:80/	health
ping	GET	http://stage-mcs-identity.cg.bskyb.com:80/mcs-identity	ping/{delay}
Identity onyx ping signed	GET	http://stage-mcs-identity.onx-sc.cg.bskyb.com:80/mcs-identity	ping/{delay}

On-boarding

Access to services authorized through OAuth standard

Management of consumers and services in Gatekeeper done through client admin application

Clients provided with key and/or secret when on-boarding

Client Management Application

User: Krishan Lakha Logout

Publish!

11:15:02 : Configuration has not been published yet

Navigation

Hosts & Endpoints

Services

Consumers

Audit

DeploymentInfo

Consumers

+ Add Consumer

Reference Name	Consumer Key	Use Unsigned Request
mcs	mcs	true

Service Reference Name	Service Method	Internet Access Enabled	Creation Date	Max Tps Limit	
entitlements	GET	false	11/07/2014	0	✕
management-properties	GET	false	11/07/2014	0	✕
profile	GET	false	11/07/2014	0	✕
entitlementsforlogin	GET	false	11/07/2014	0	✕
extendedLoginProfile	GET	true	11/07/2014	0	✕
extendedLoginProfile-e04	GET	false	11/07/2014	2	✕
health	GET	true	11/07/2014	0	✕
oogway-profile	GET	true	22/07/2014	2	✕
management-vcapapplication	GET	false	11/07/2014	0	✕
ping	GET	true	11/07/2014	0	✕

Grant Consumer Service Access

sky.com

\\(c\$0jnNgZ3AKYJz/D')Js|x<x')8l)Rs

true

Why expose MCS on the Internet?

- More clients are using external cloud services to host their applications
 - e.g. AWS, Heroku etc.
- These applications still have to serve Sky customers
 - Often means needing access to confidential/secret customer data
 - Data security issues
 - PCI concerns
- Gatekeeper can provide secure entry to MCS and different Sky systems
 - Secure transport
 - Validation and authentication



What can Gatekeeper do for you?



What Gatekeeper can do for clients

- Provides secure internet/intranet access to services deployed internally within applications hosted in Sky Datacentres
 - Signed requests using key and secret
 - Unsigned requests with key and Oogway token
- Secure communication over HTTPS
 - Trusted Verisign cert in place
- Minimal overhead on service response times
- Unified entry point to services
- High availability
 - Deployed in Nimbus CloudFoundry
 - Create more instances on demand
 - Multiple data centres for DR
- Simple transformation of service response to suit client requirements
 - e.g. JSONP
- In production with one client



What Gatekeeper can do for service providers

- Gives you access control over your services
 - Allow access to known clients only
- Protect downstream systems by rate limiting access to back-end services
 - Service quota decided with client
 - Requests exceeding quota are rejected at Gatekeeper
 - Prevents misuse and reduces the risk of outages
- Separation of concerns (security)
 - Secure transport handled via HTTPS
 - SSL terminated at Gatekeeper
 - No need to worry about certificates, key pairs etc.

Next steps

- Provide HTTP access to existing JMS-over-MQ services
- Timestamp & nonce support for additional repeat attack protection
- Analytics & Traffic monitoring
- Data transformation & mapping
- Self-serve model for accessing services
- Support for more RESTful APIs (PUT, POST, DELETE etc.)
- ...

