



**smith**  
secure access made easy

**When trying to manage access to systems and data we are faced with unsatisfying trade-offs.**



**Do we over-protect? Securing systems at  
the cost of usability and productivity.**



**Do we over-provision access? Ensuring  
access at the cost of security and confidence.**



**Trying to balance these concerns is not feasible  
when we think of access as all or nothing.**

**Do we grant access or don't we?**



**We want to be able to manage access control in terms of **when** and **how** someone has access, not just **what** they have access to.**



**Access control should be  
time and workflow sensitive.**



# Ephemeral Access with SSH Certificates





What is the **danger** of a stolen SSH key?



**How many keys and users have access to  
your systems right now?**



**How many are actually accessing those  
systems right now?**





POSTED ON SEP 12, 2016 TO [PRODUCTION ENGINEERING](#), [SECURITY](#)

## Scalable and secure access with SSH

<https://code.fb.com/production-engineering/scalable-and-secure-access-with-ssh/>

The Netflix logo, the word "NETFLIX" in red, bold, sans-serif capital letters on a black background.

**NETFLIX**

A dark presentation slide with white text. The background shows a blurred image of a person's hands on a laptop keyboard. The text reads: "How Netflix Gives All Its Engineers SSH Access To Instances Running In Production".

How Netflix Gives All Its Engineers SSH  
Access To Instances Running In Production

<https://speakerdeck.com/rlewis/how-netflix-gives-all-its-engineers-ssh-access-to-instances-running-in-production>



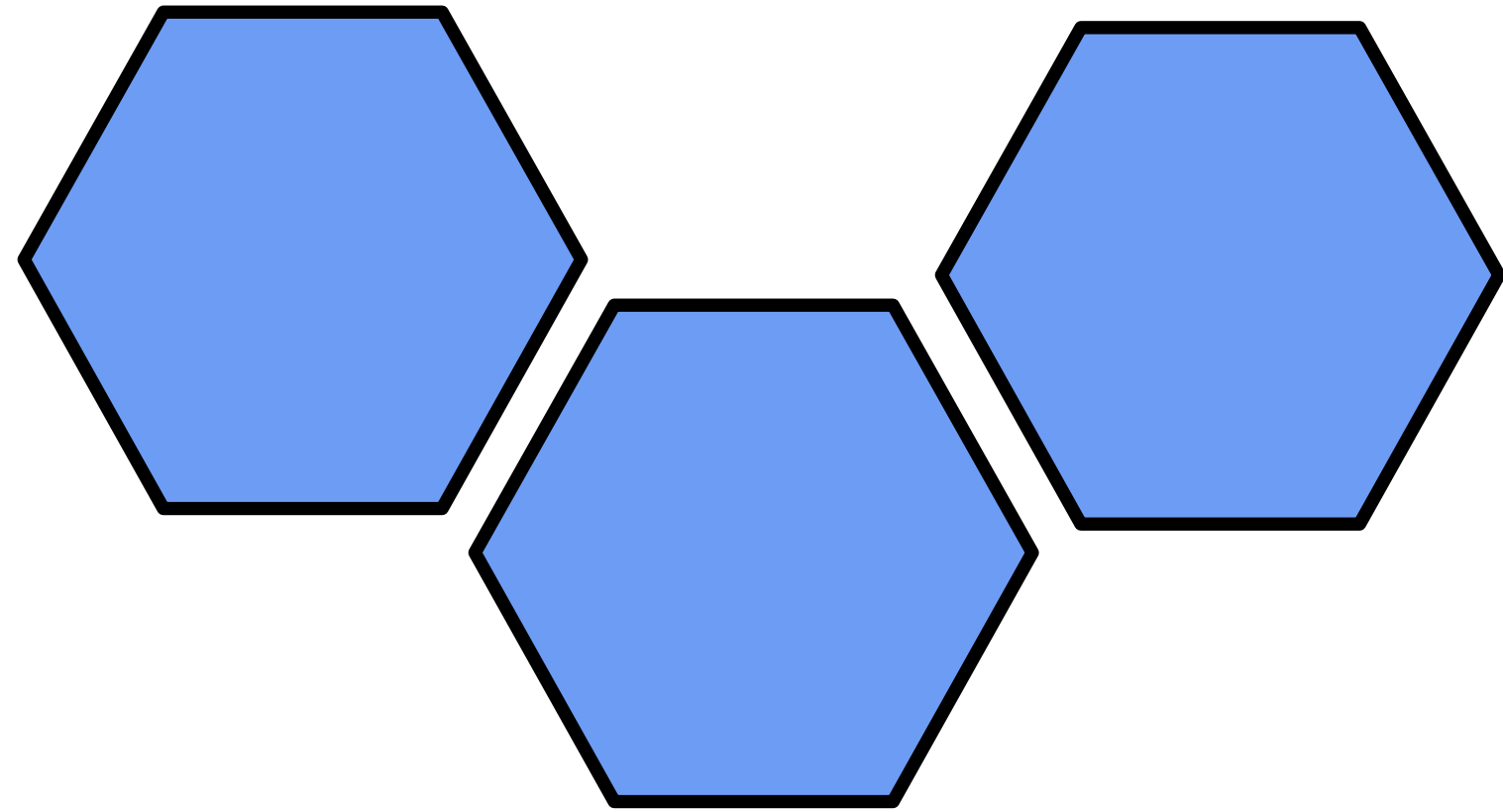
**smith**  
secure access made easy

**How does it work?**

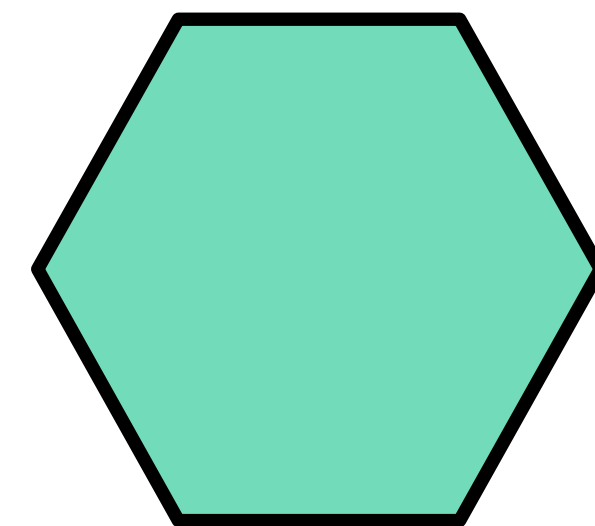
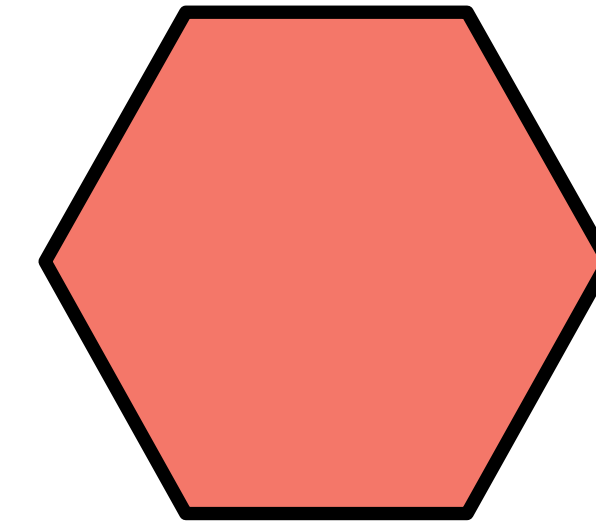




**Your servers.**



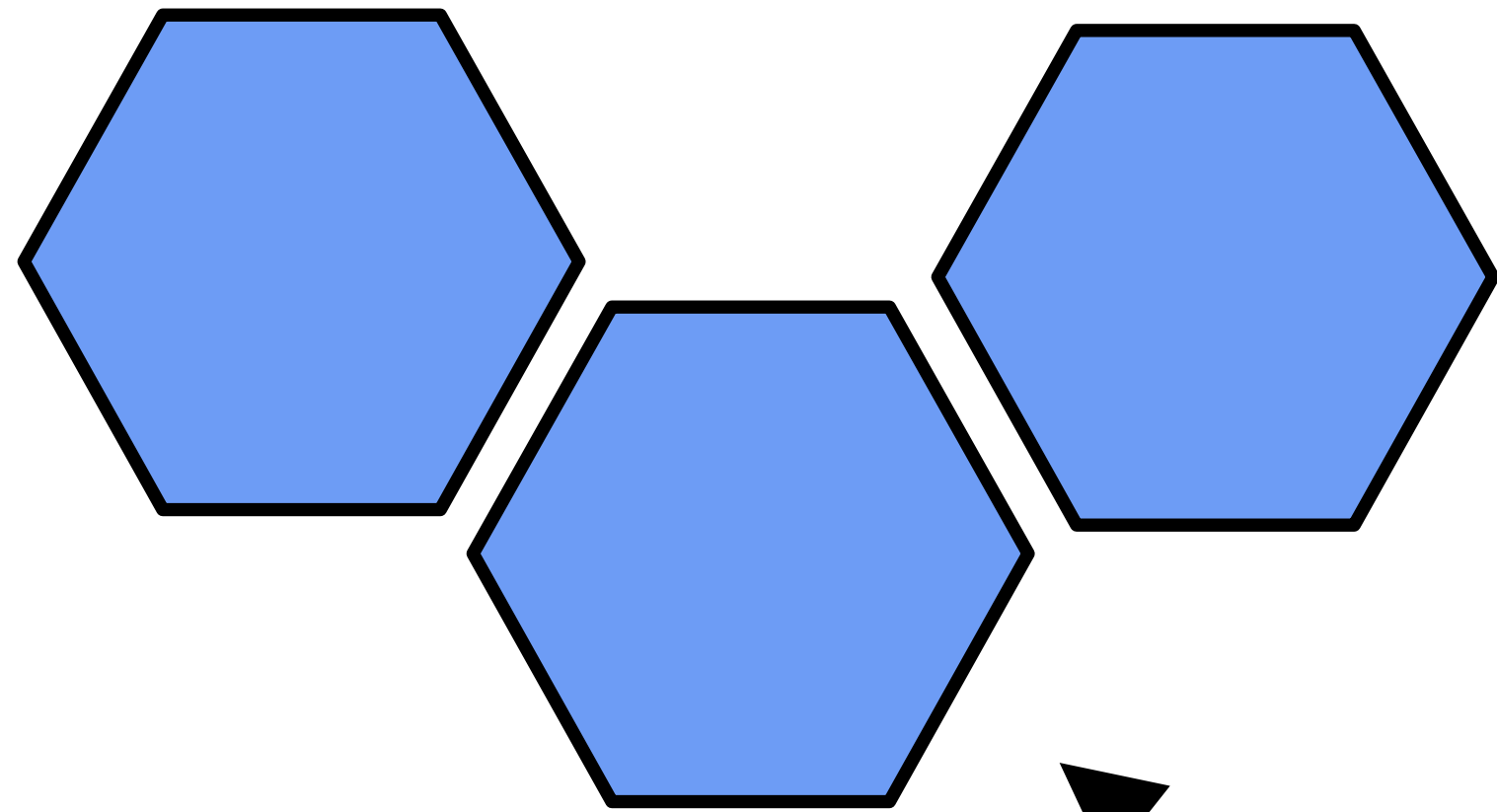
**Certificate authority.**



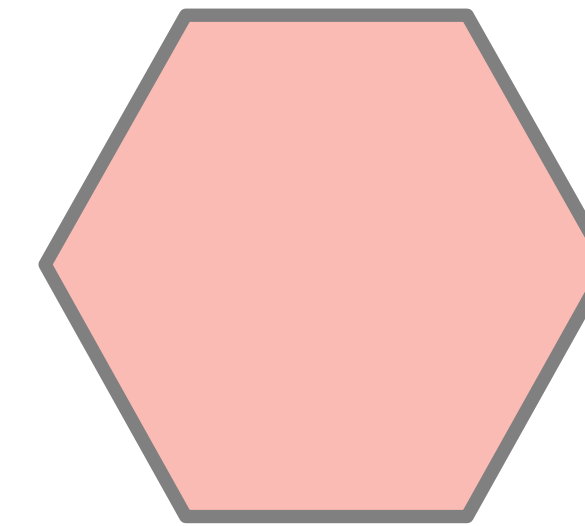
**You.**



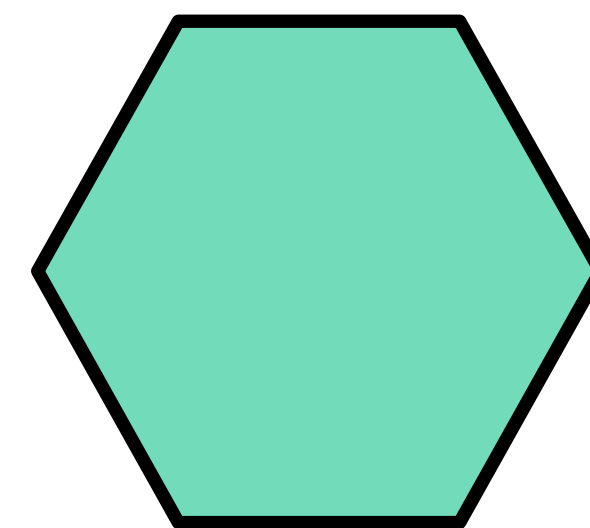
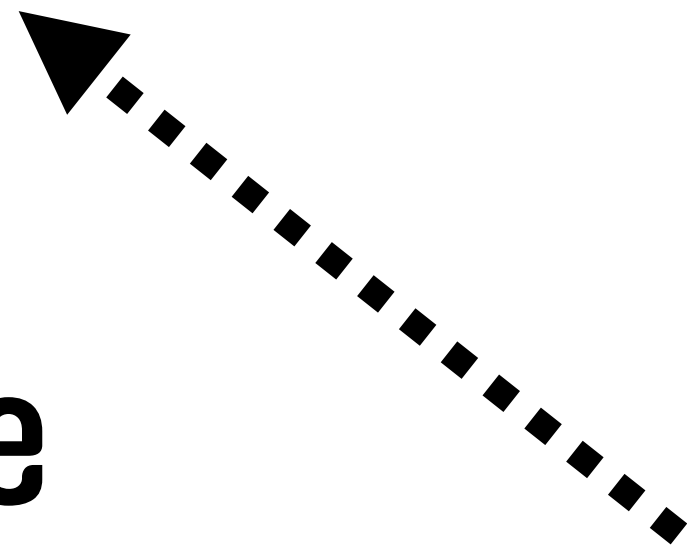
**Your servers.**



**Certificate authority.**



**You don't have  
persistent access to  
servers.**

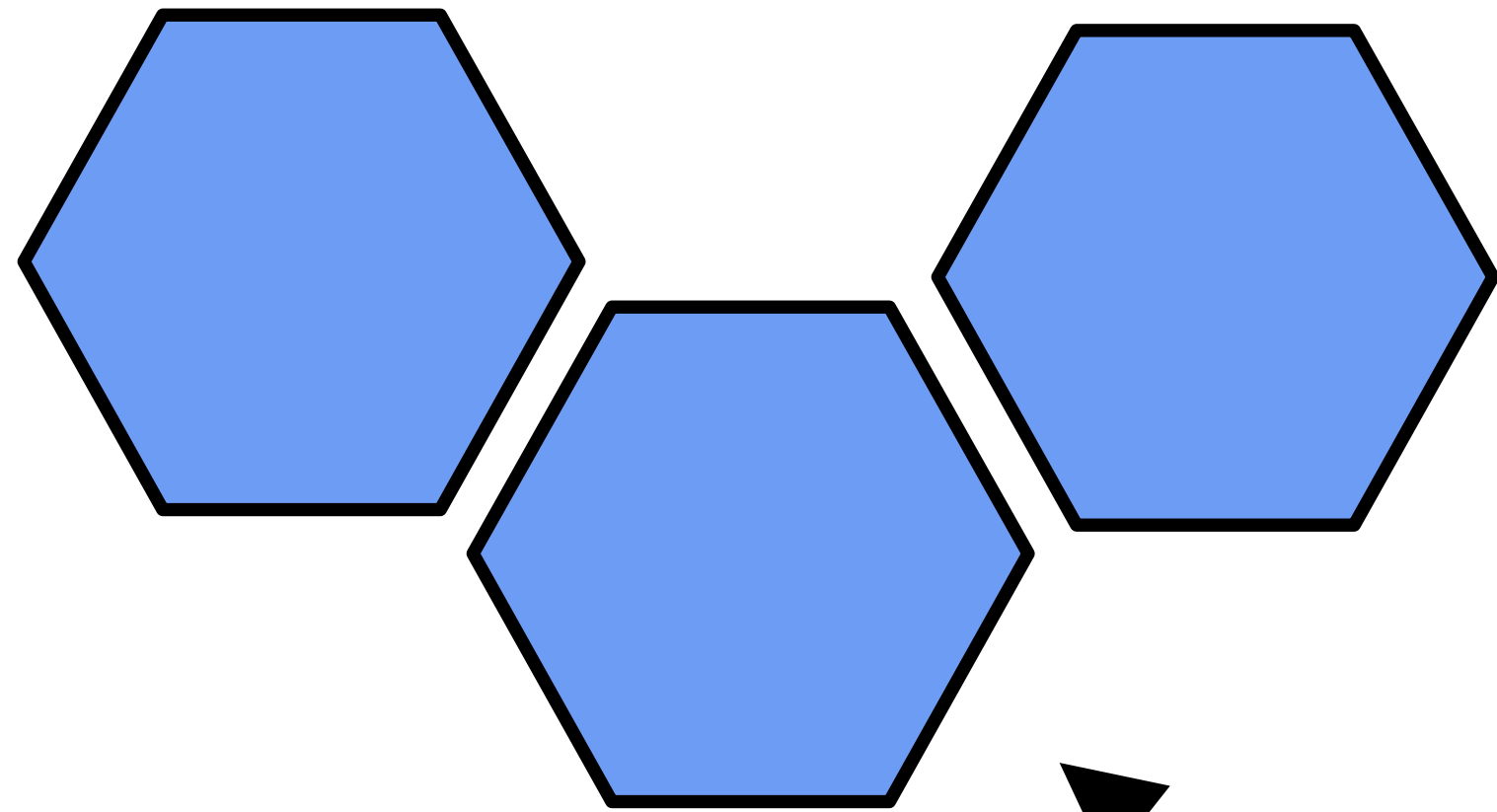


**You.**

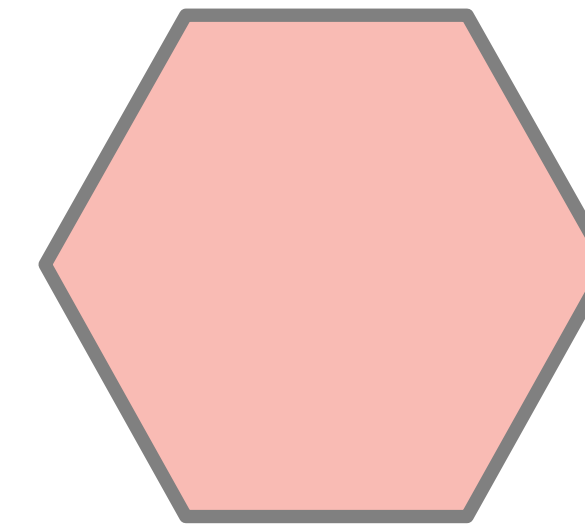




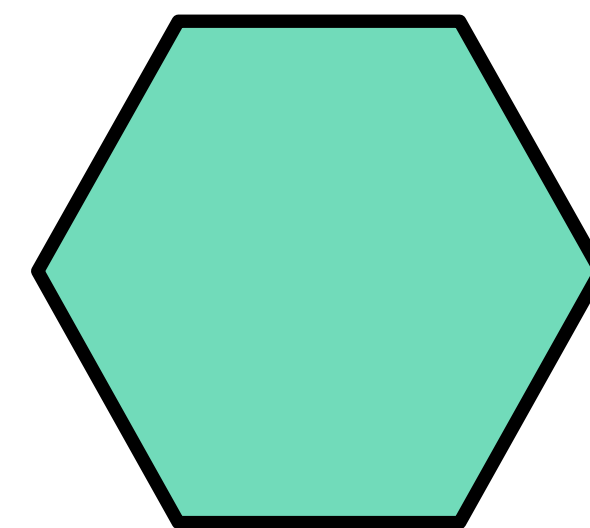
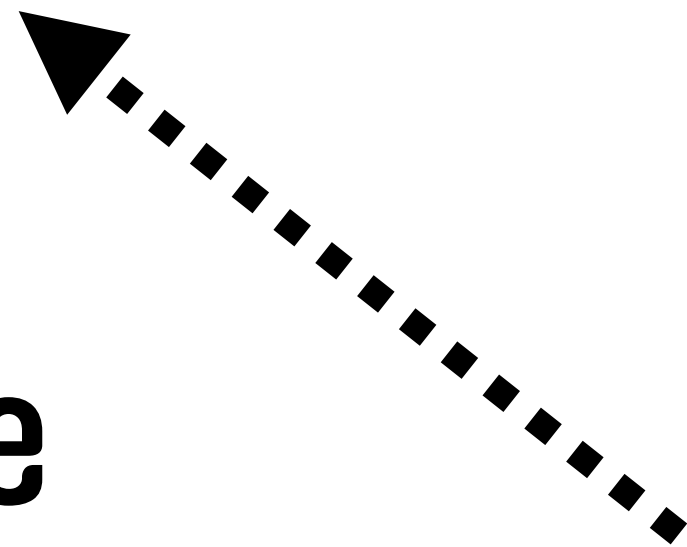
**Your servers.**



**Certificate authority.**



**You don't have  
persistent access to  
servers.**



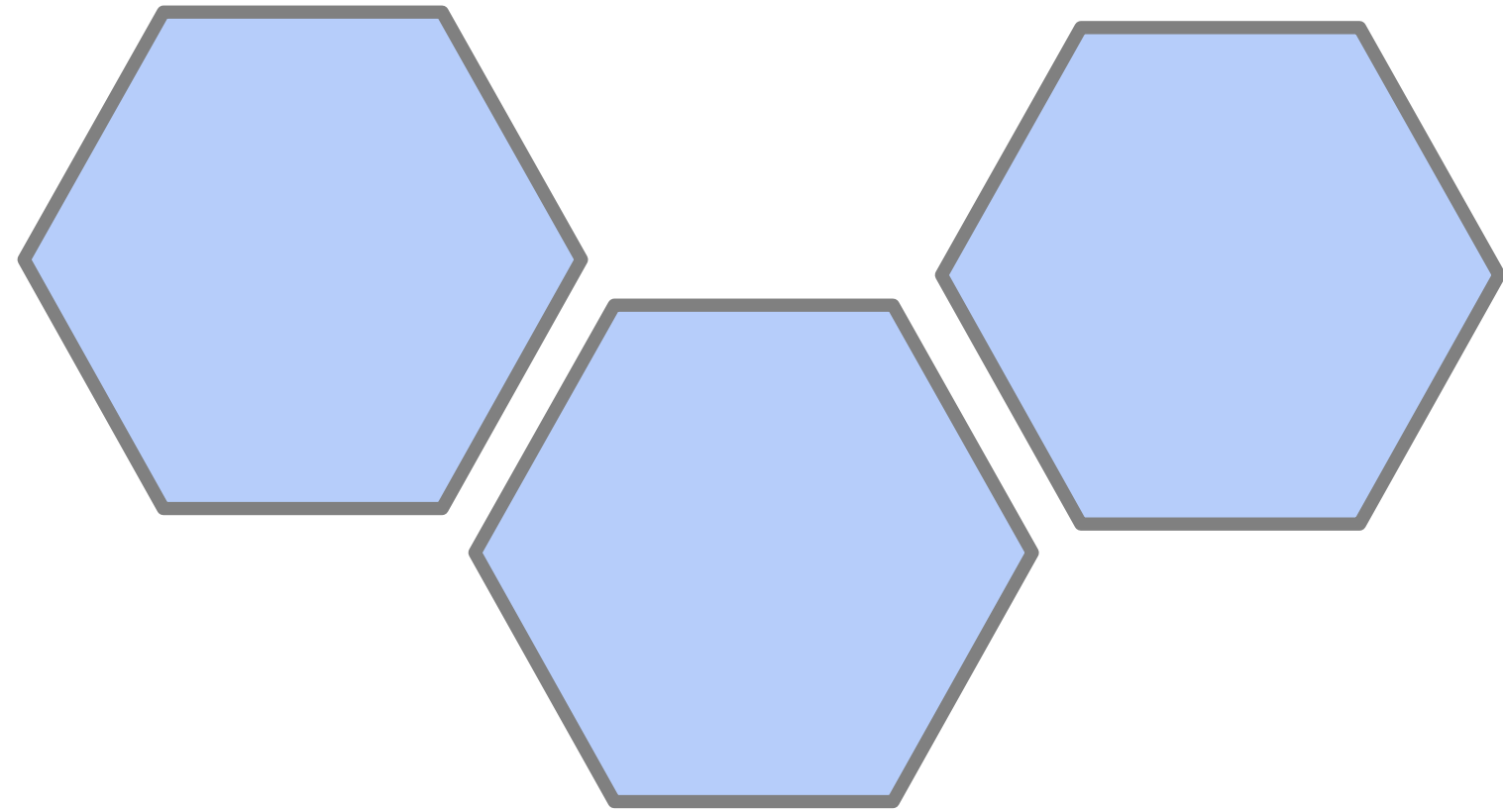
**You.**



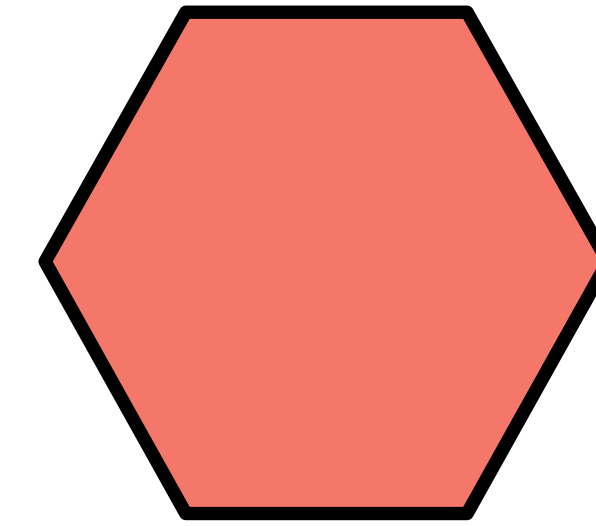
**This means minimising risk of  
leaked SSH credentials from  
developers and operations.**



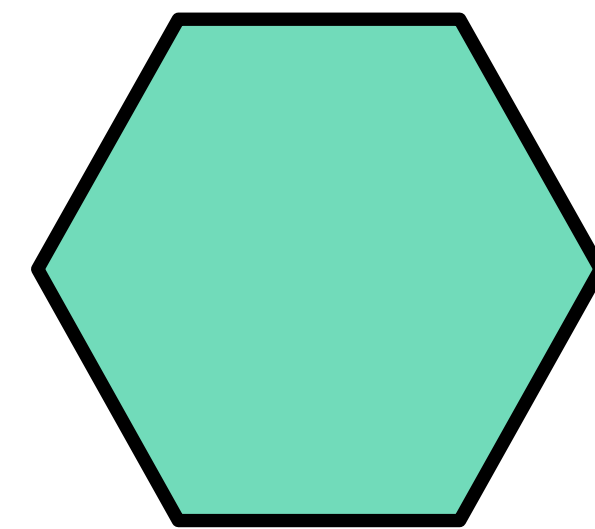
**Your servers.**



**Certificate authority.**



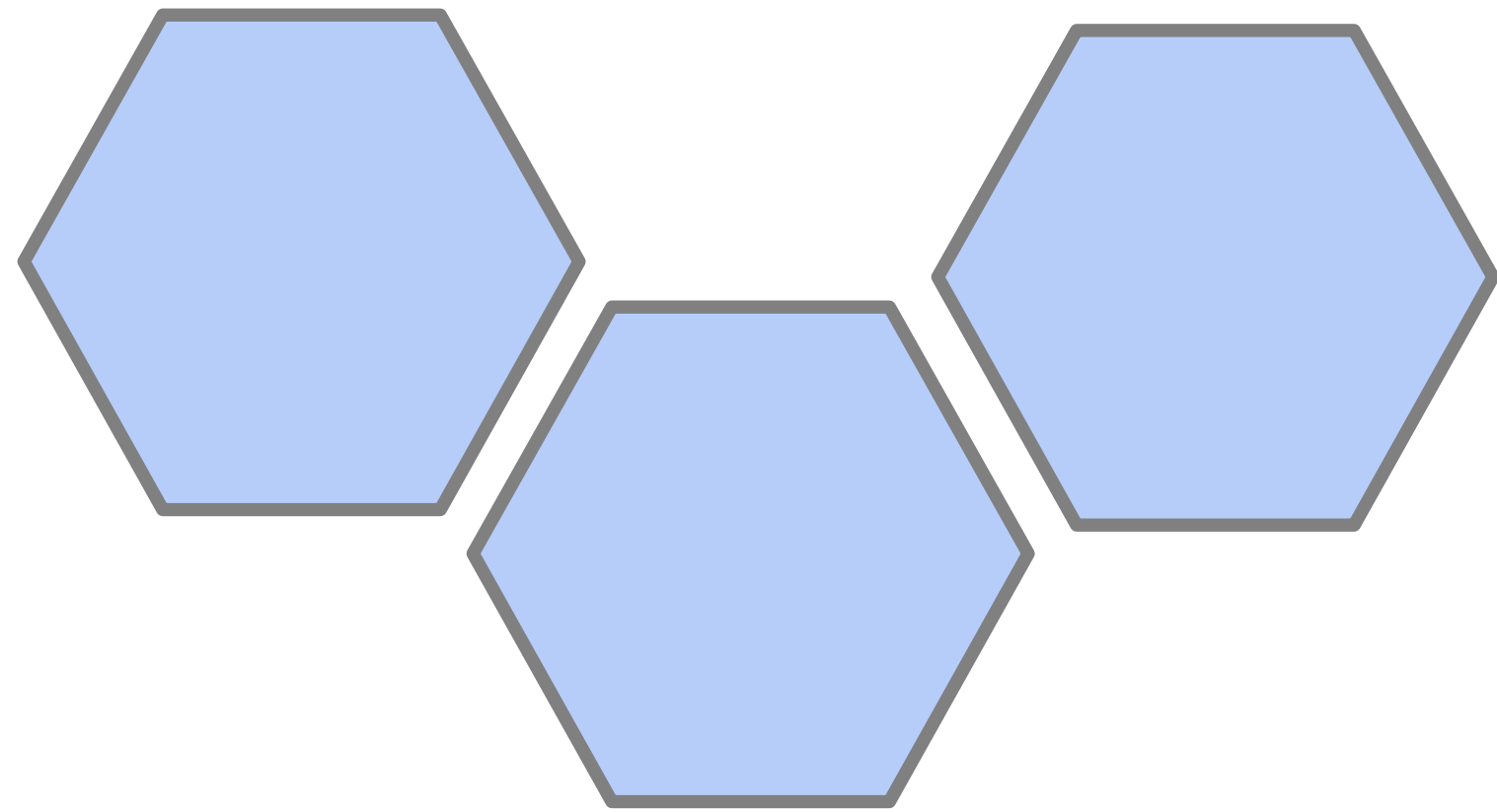
**Request server access  
on demand as a part of  
your workflow.**



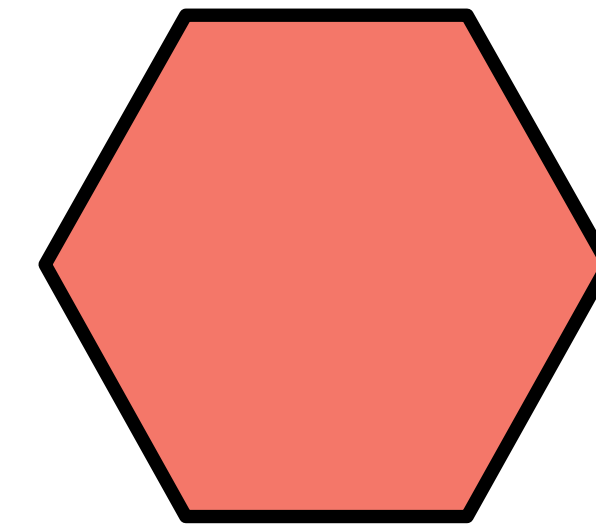
**You.**



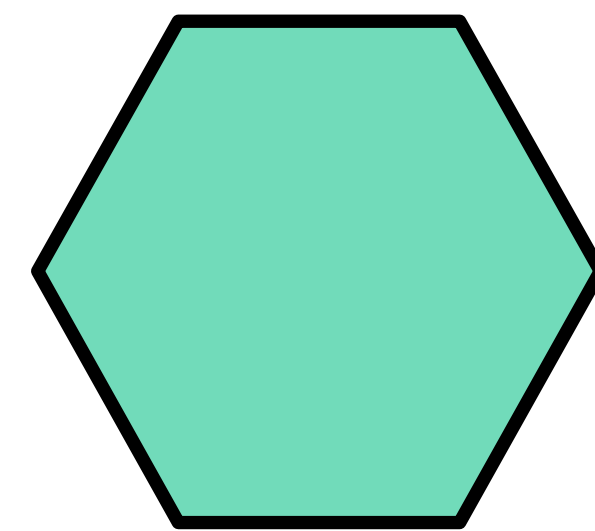
Your servers.



Certificate authority.



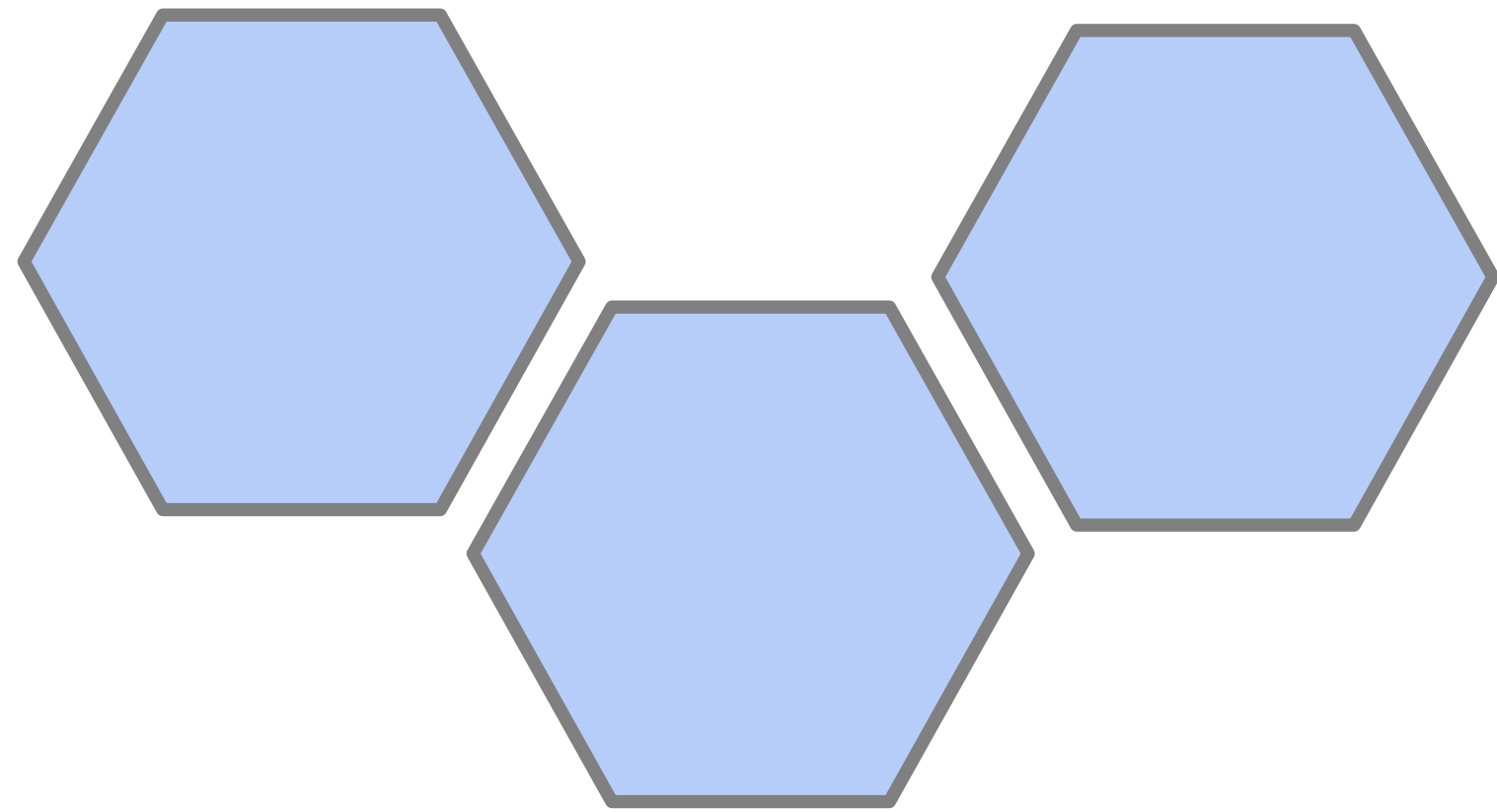
Authority authenticates you, verifies that you have access and performs contextual checks.



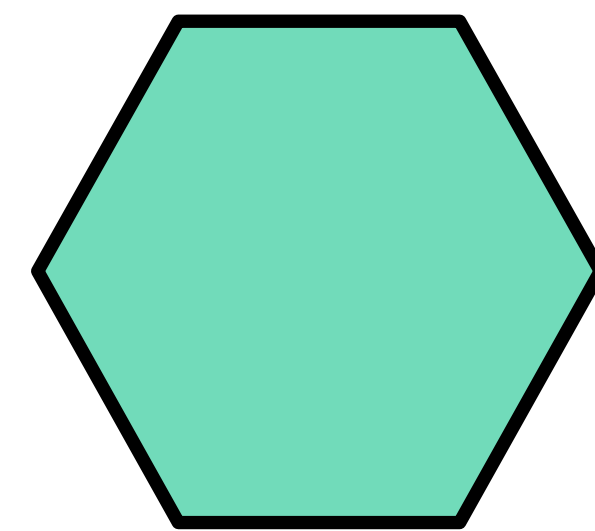
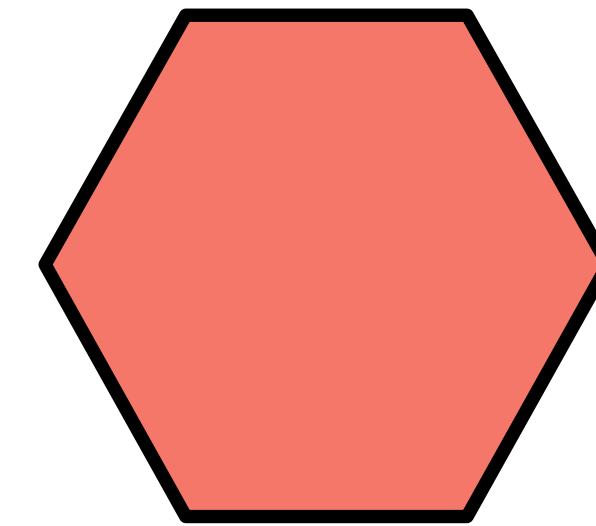
You.



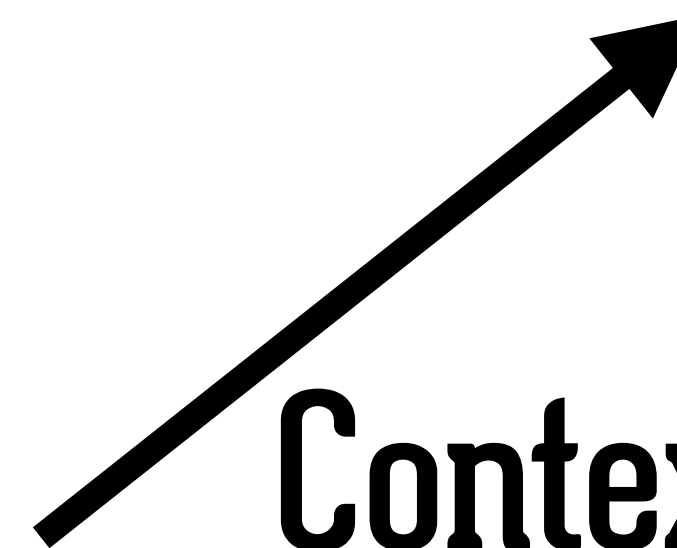
**Your servers.**



**Certificate authority.**



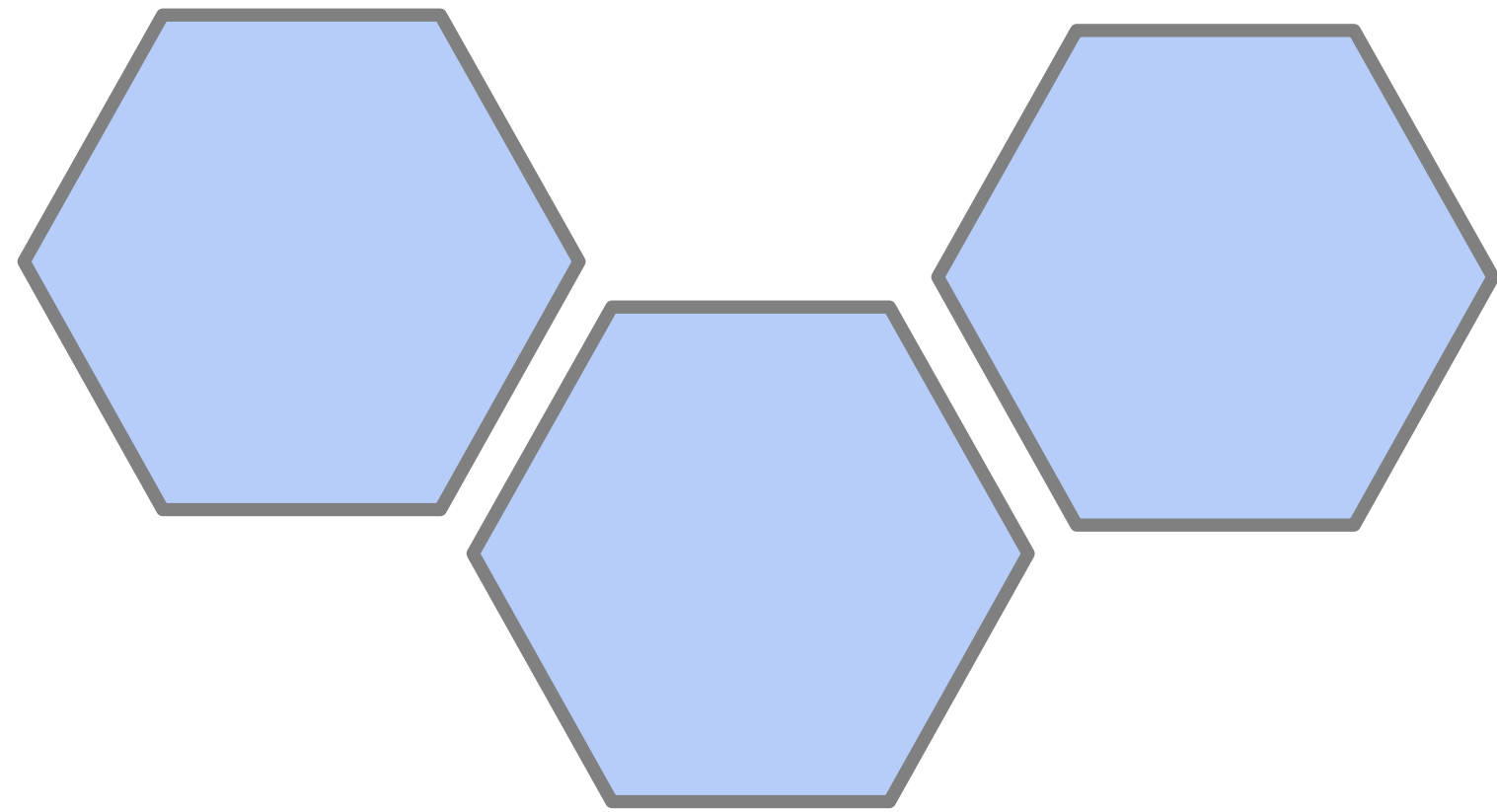
**You.**



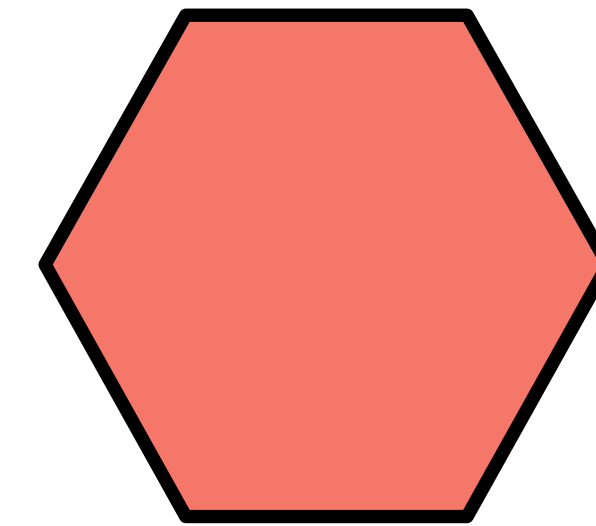
**Contextual checks may be  
your location, network  
checks, external  
approvals.**



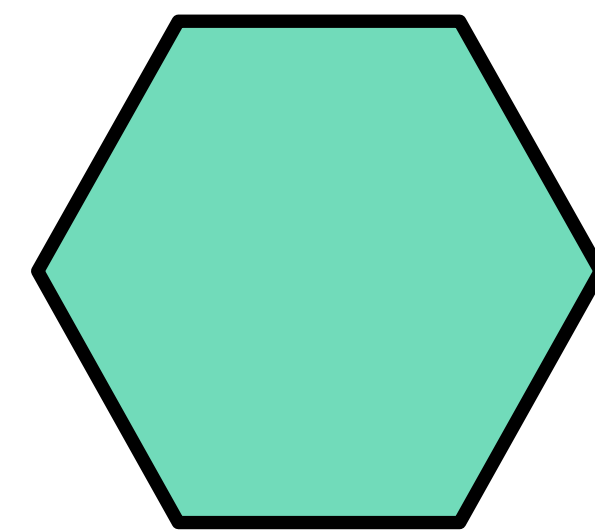
**Your servers.**



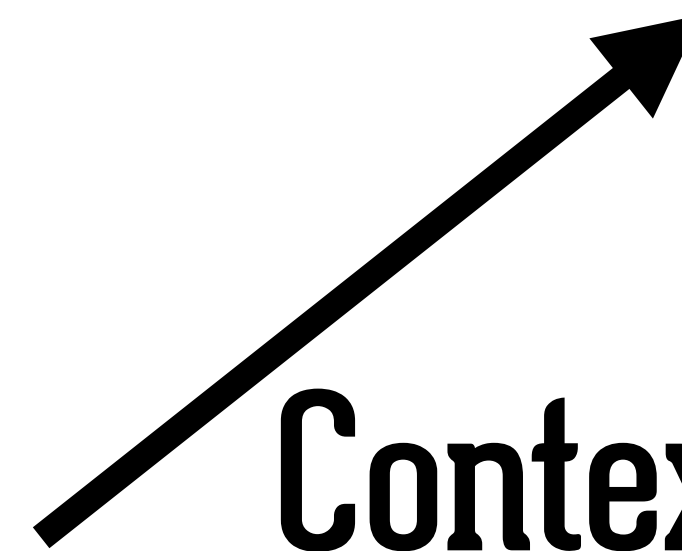
**Certificate authority.**



**Context means we can provide more meaningful access control options.**



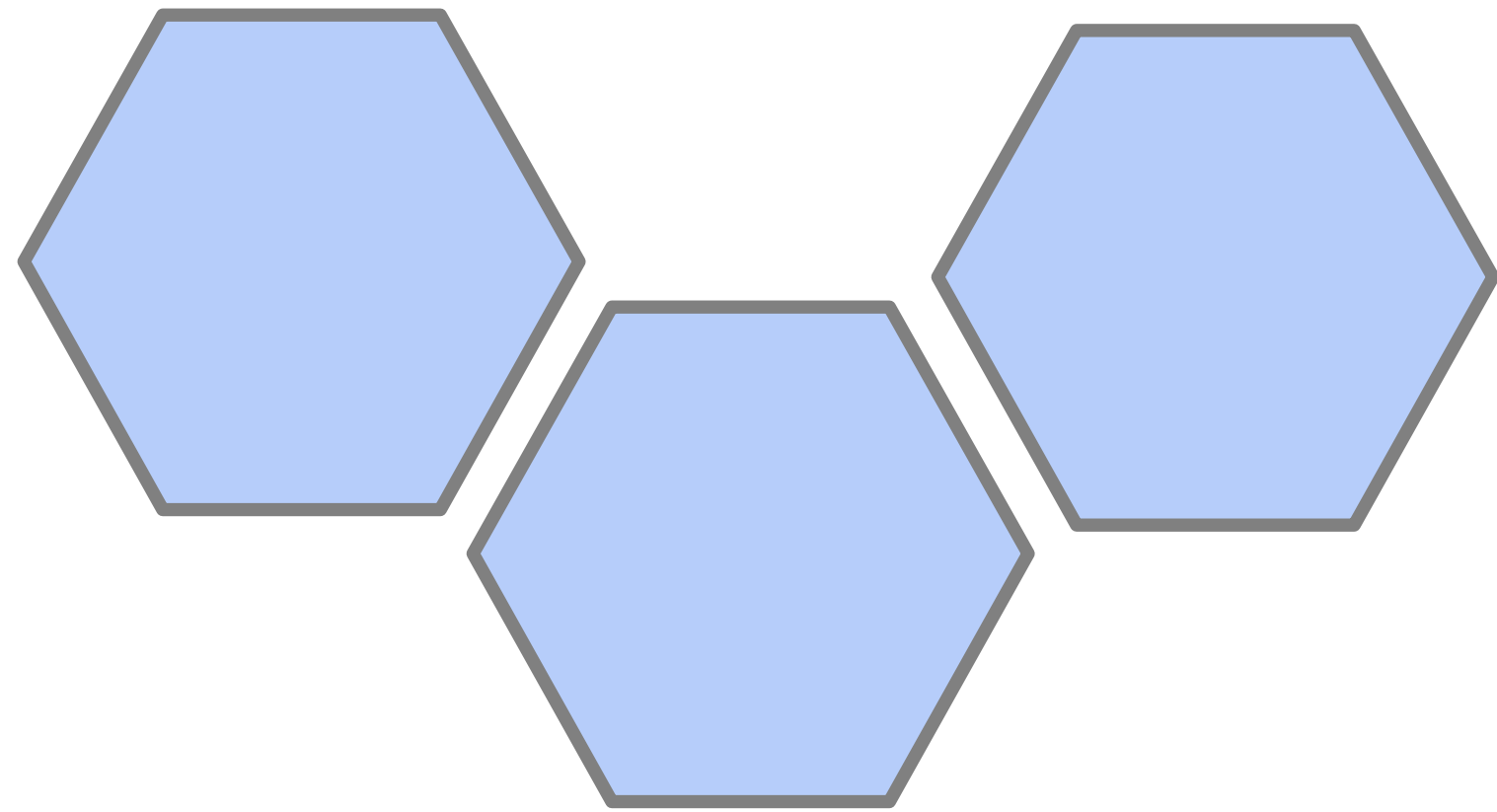
**You.**



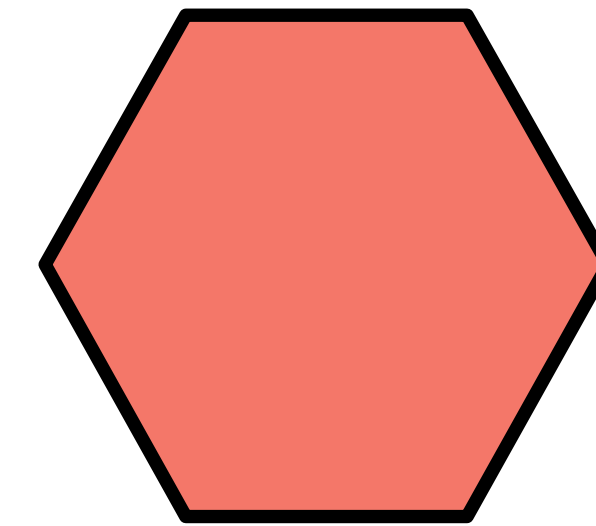
**Contextual checks may be your location, network checks, external approvals.**



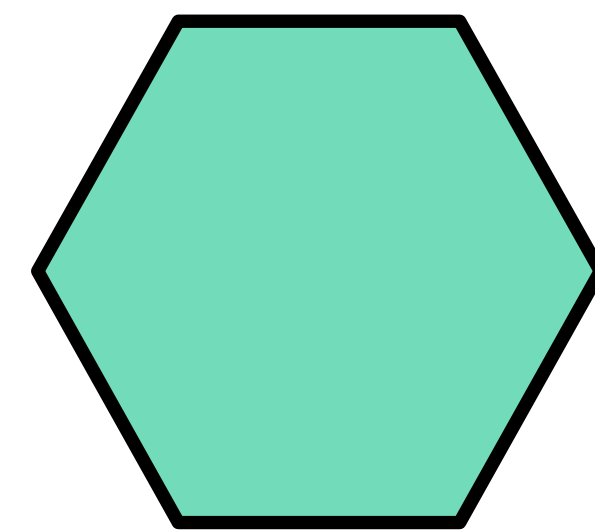
**Your servers.**



**Certificate authority.**



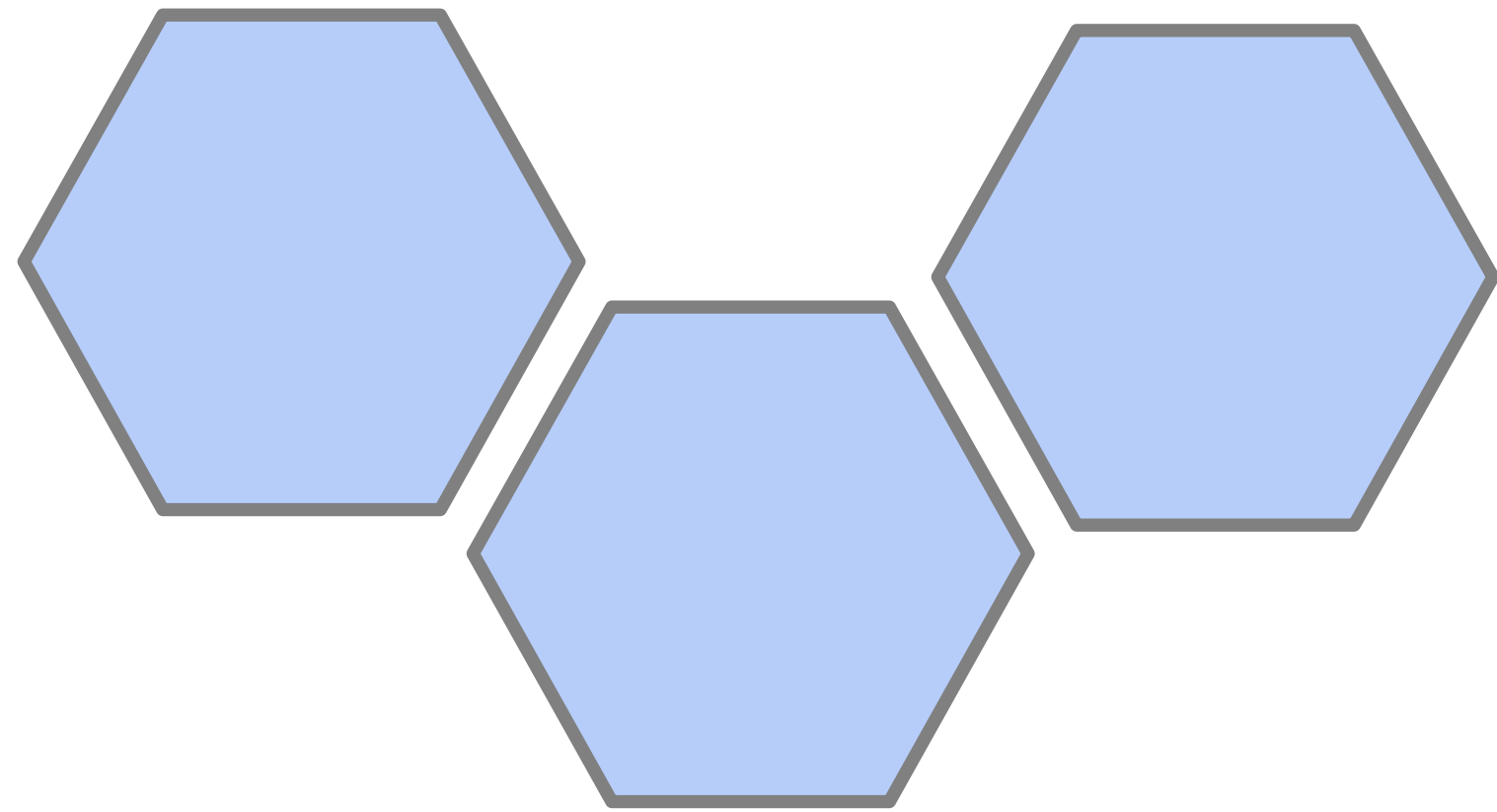
**Authority issues a  
certificate for a single use  
key, just for this task.**



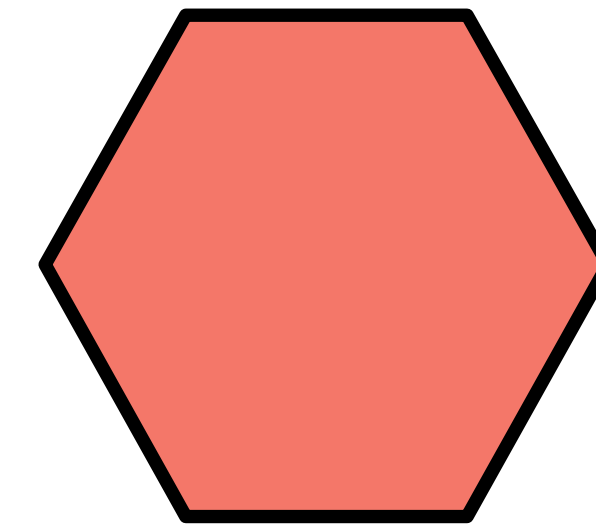
**You.**



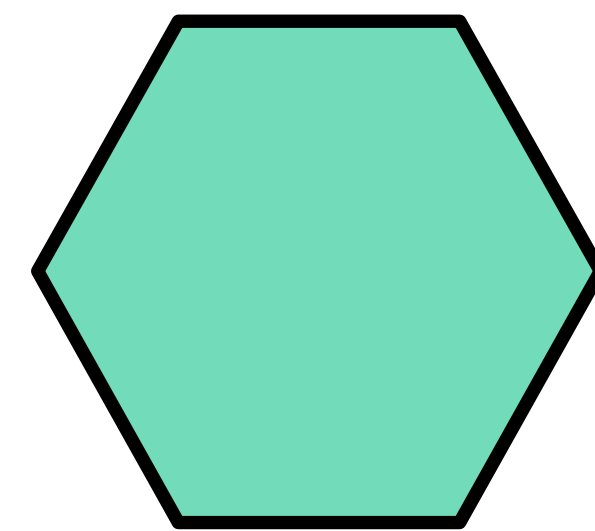
Your servers.



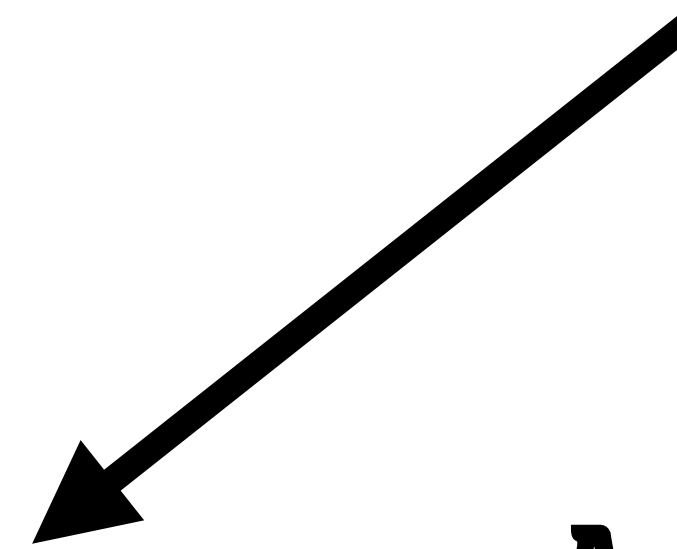
Certificate authority.



This limits the scope of our access for this request, and allows us to audit when and why access was requested.



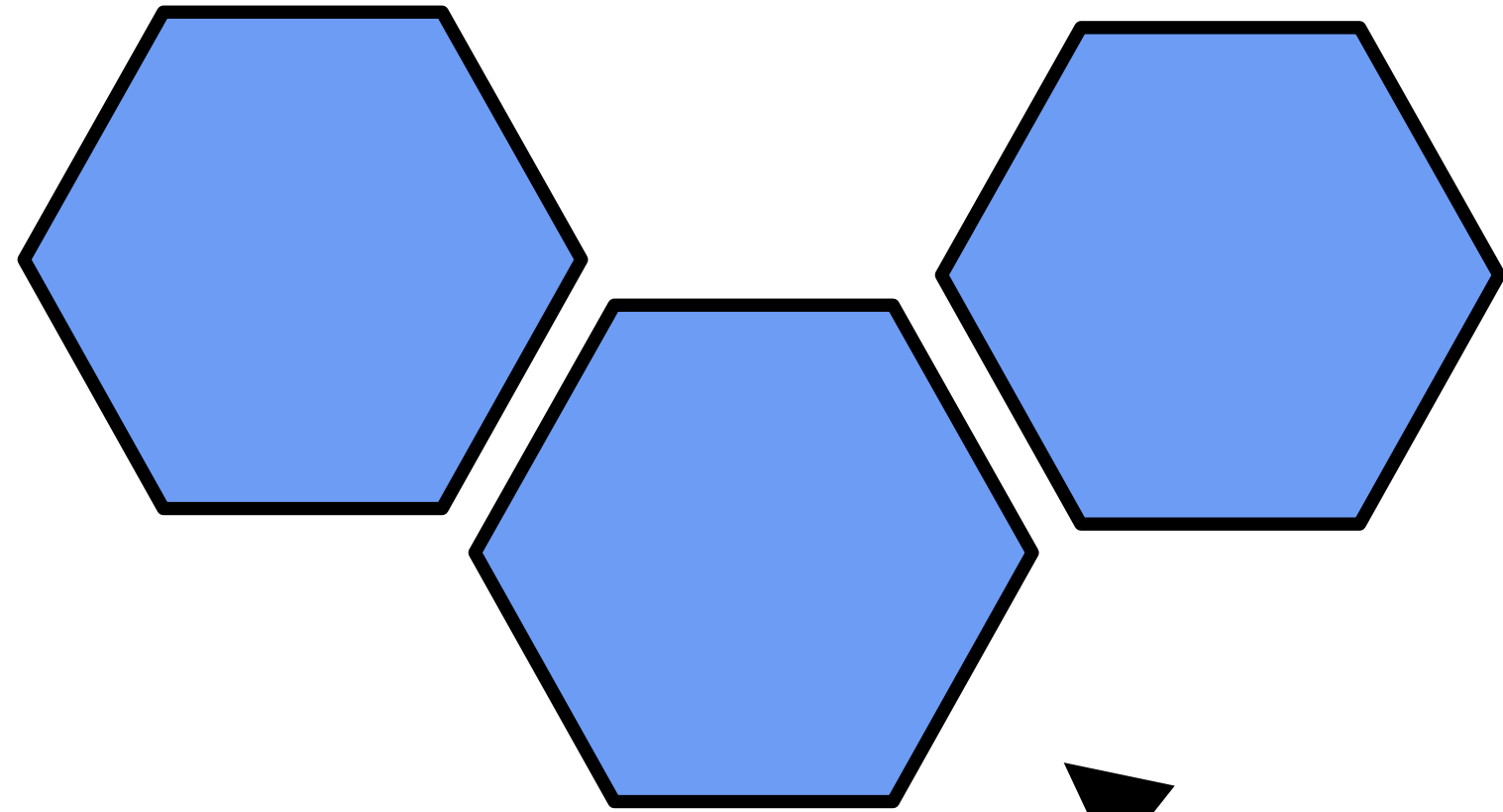
You.



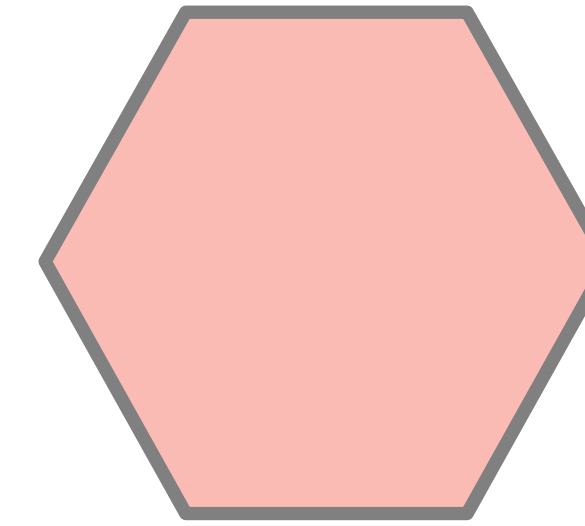
Authority issues a certificate for a single use key, just for this task.



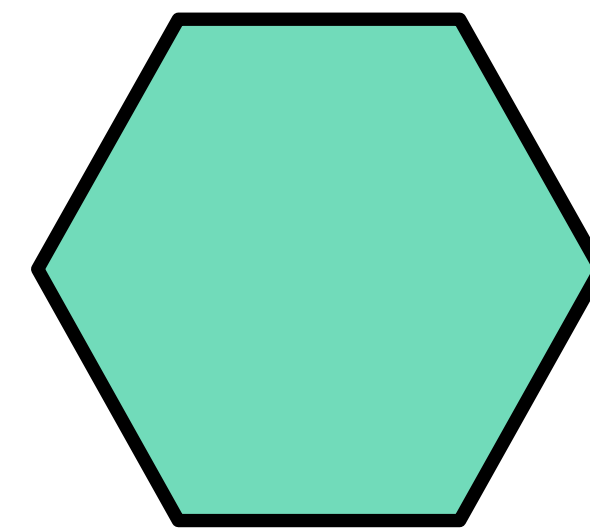
**Your servers.**



**Certificate authority.**



**Your short-lived  
credentials will provide  
you access to your  
servers.**



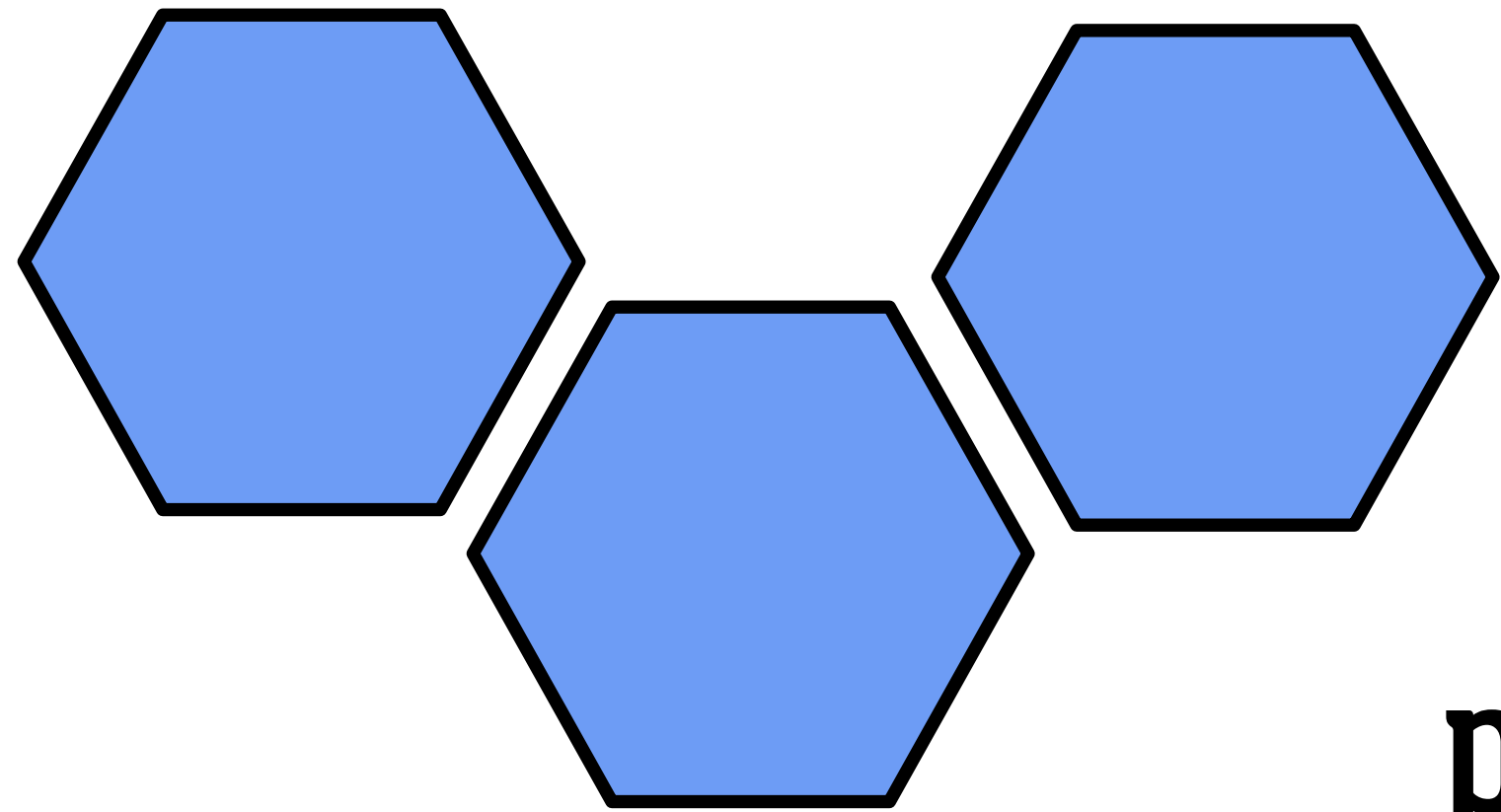
**You.**



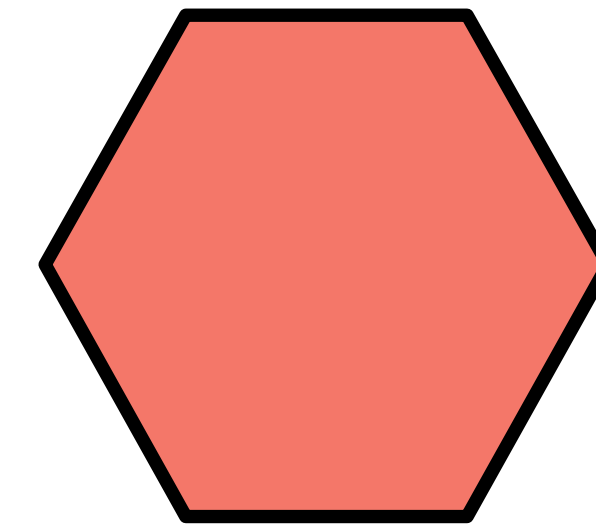




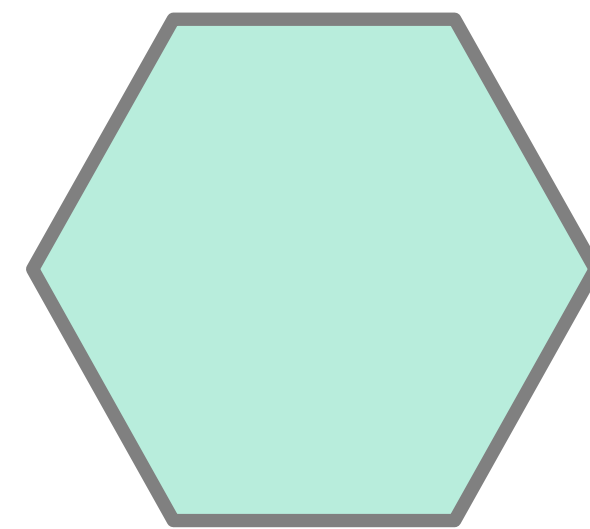
**Your servers.**



**Certificate authority.**



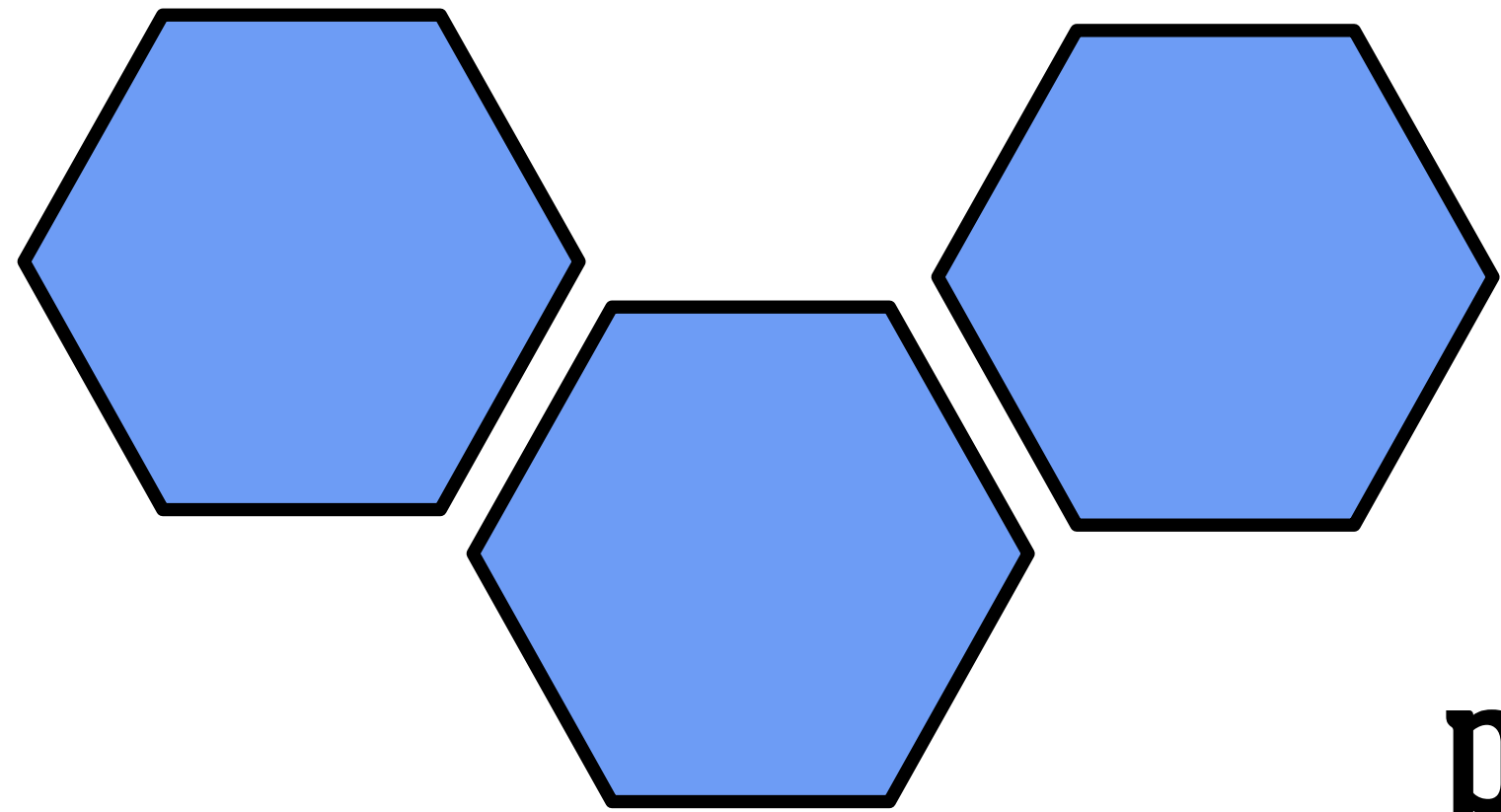
**Your servers trust  
public key of authority.**



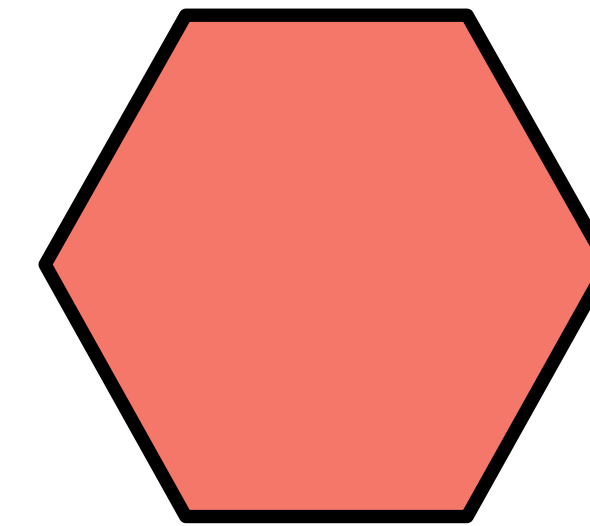
**You.**



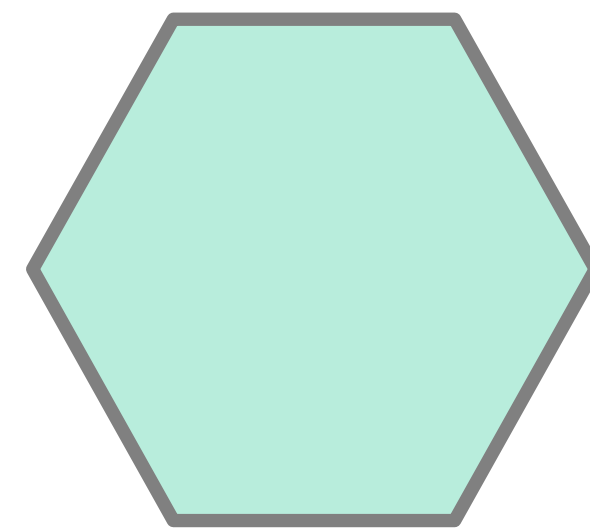
**Your servers.**



**Certificate authority.**



**Your servers trust  
public key of authority.**



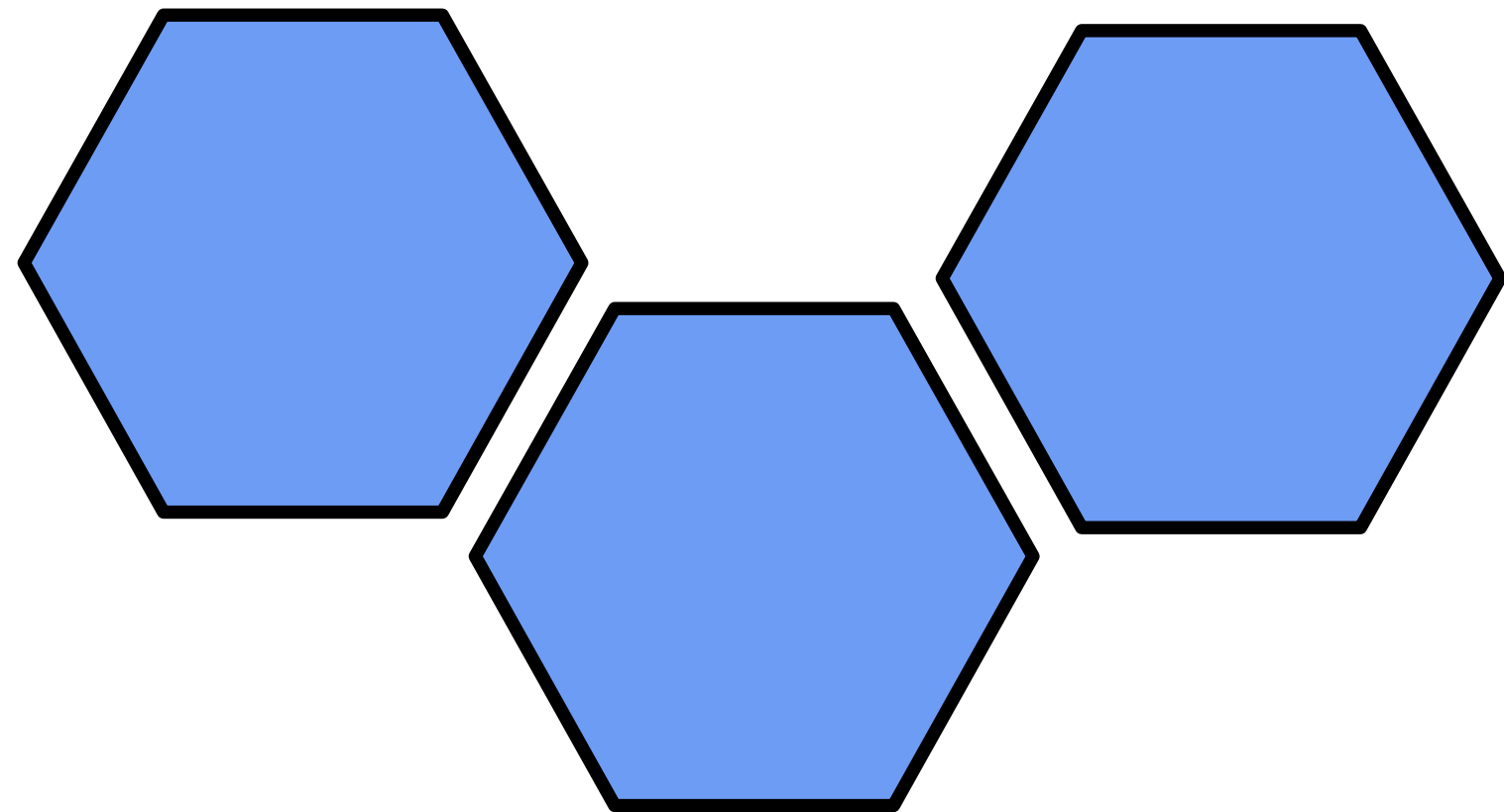
**You.**



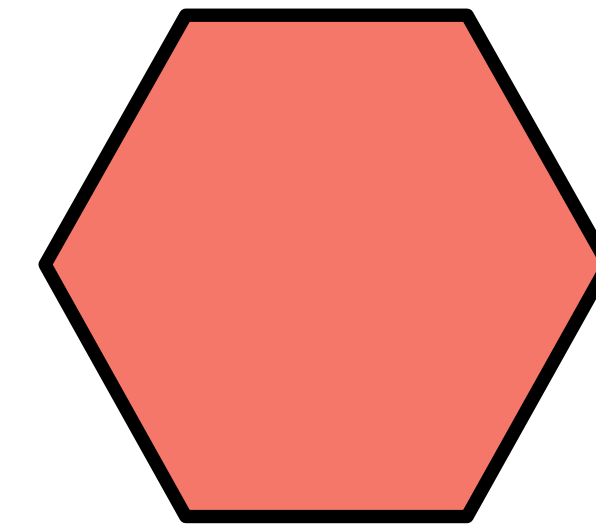
**This means no per server  
configurations that often  
complicate cloud deployments.**



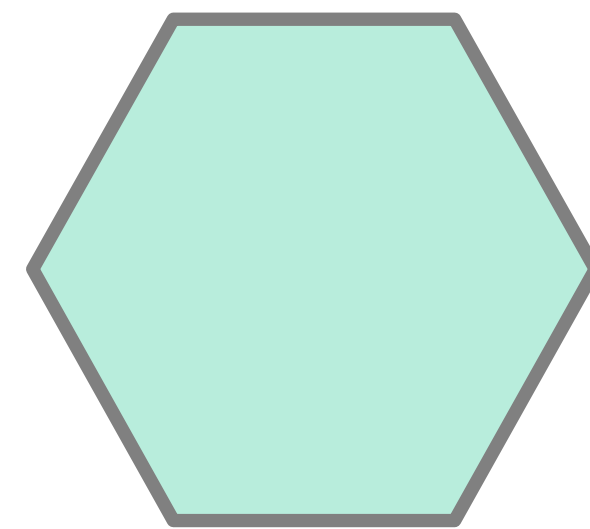
**Your servers.**



**Certificate authority.**



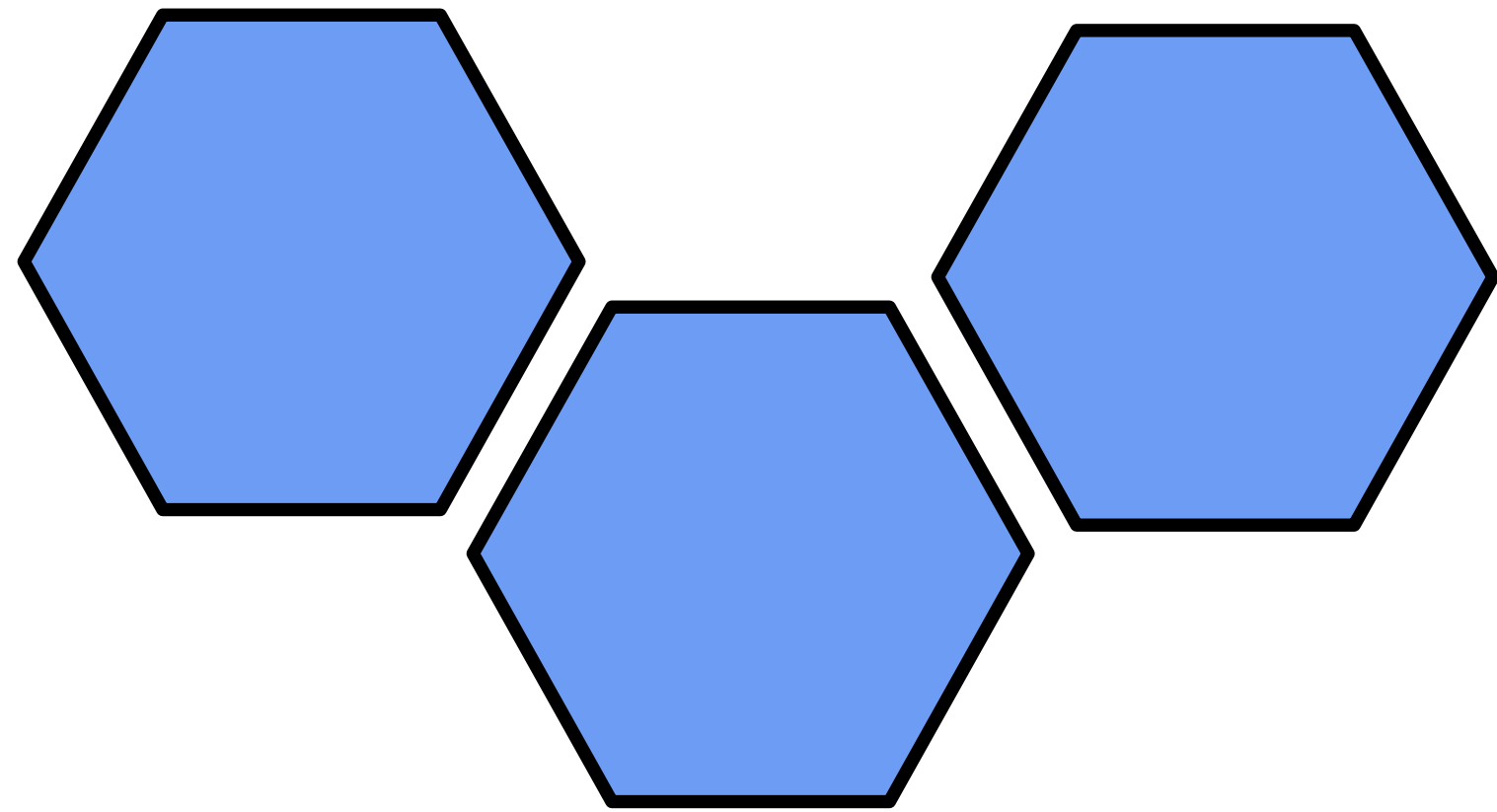
**No active network  
connection required.**



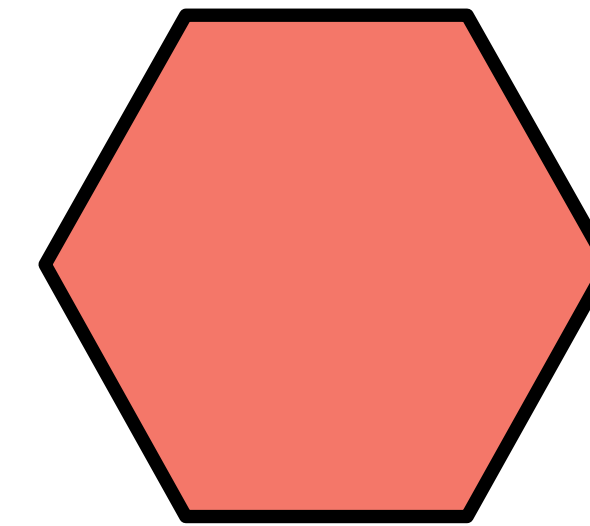
**You.**



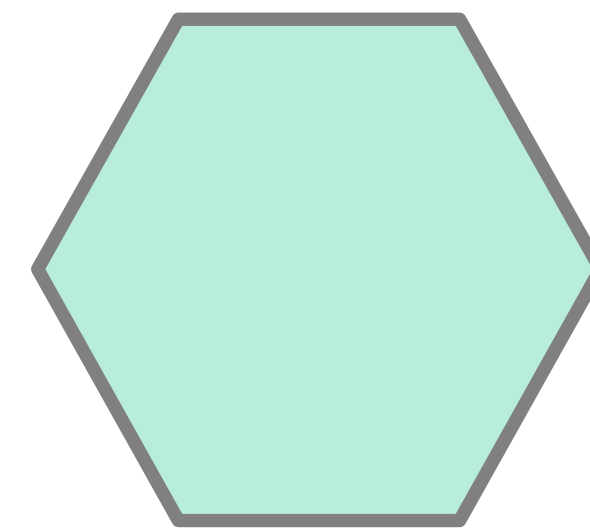
**Your servers.**



**Certificate authority.**



**No active network  
connection required.**



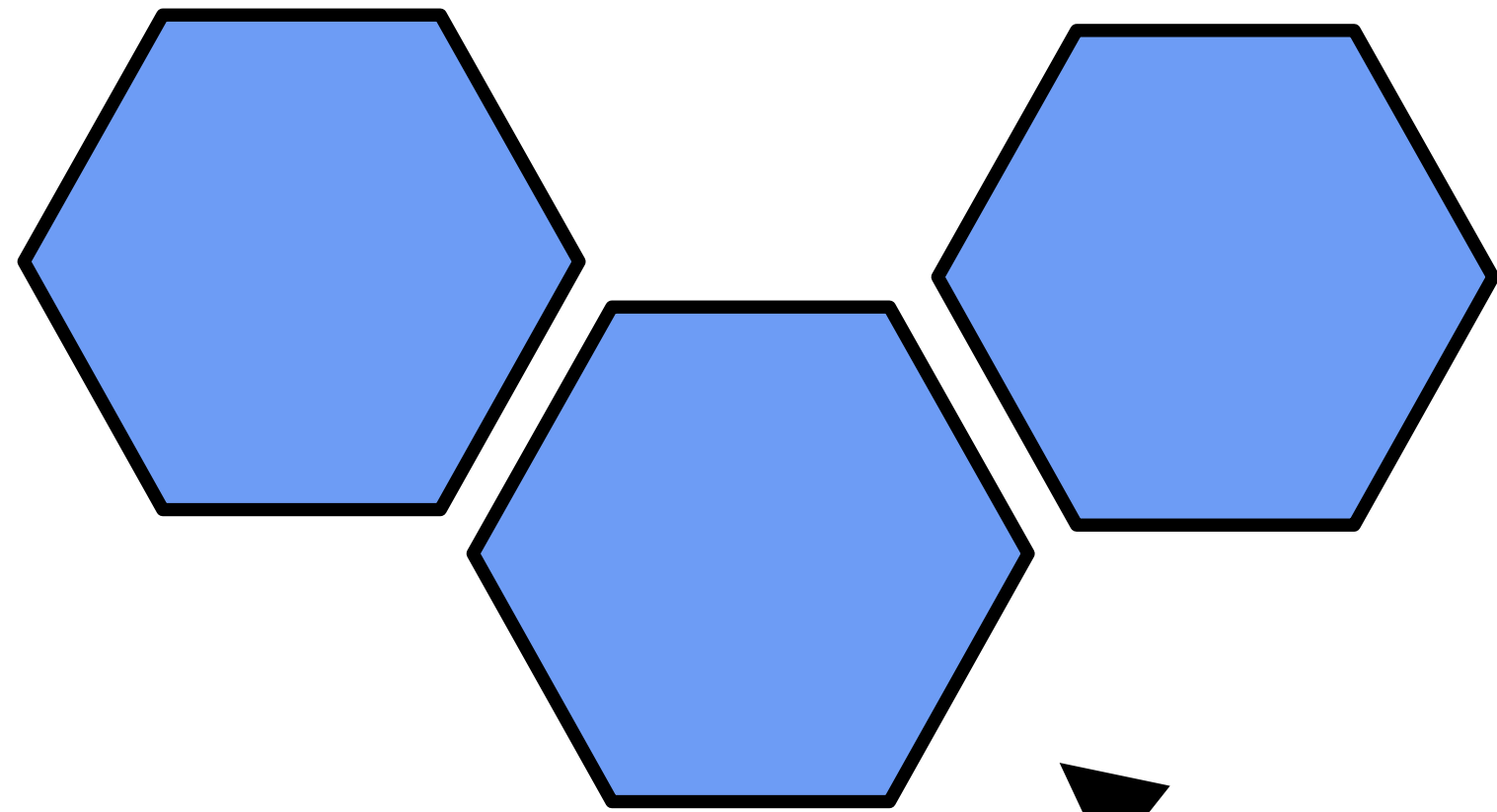
**You.**



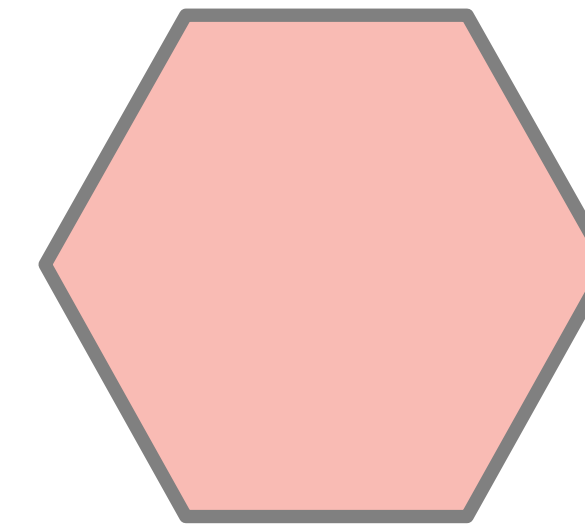
**This means reliability and no  
risk of authentication services  
impacting production.**



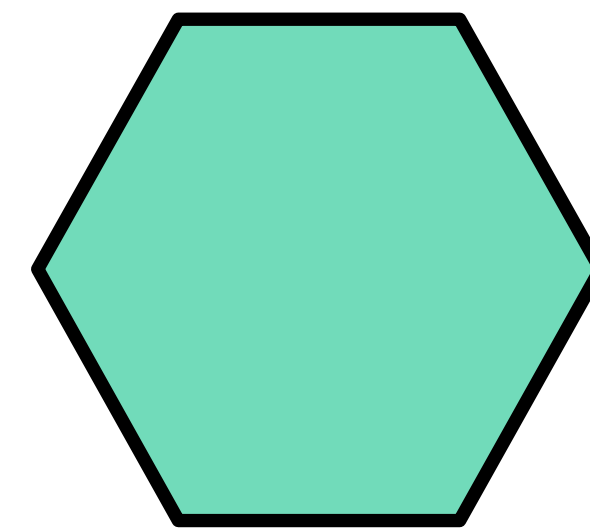
**Your servers.**



**Certificate authority.**



**Certificate attributes  
can be used to limit  
access to specific  
servers or purposes.**

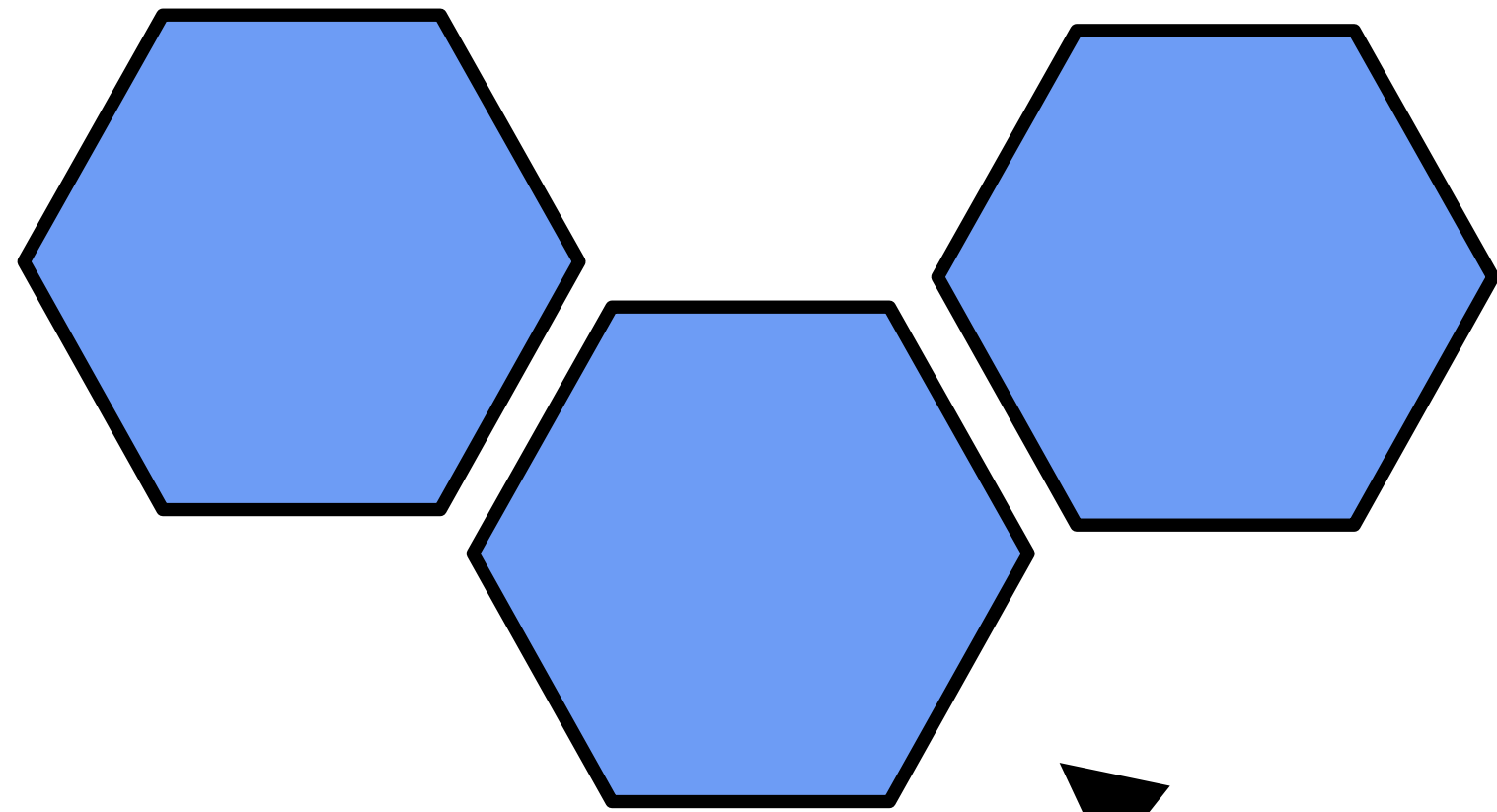


**You.**

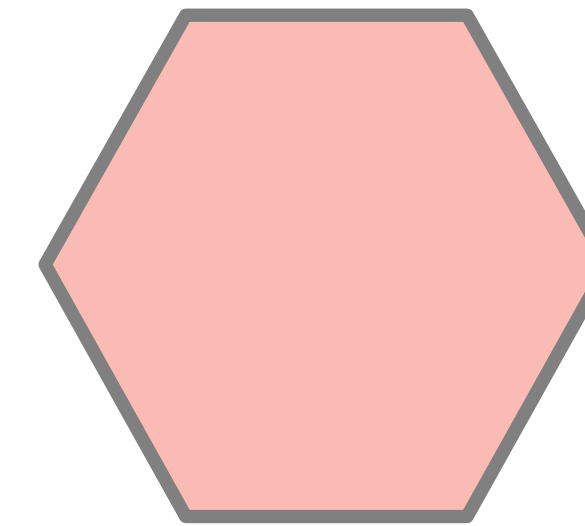




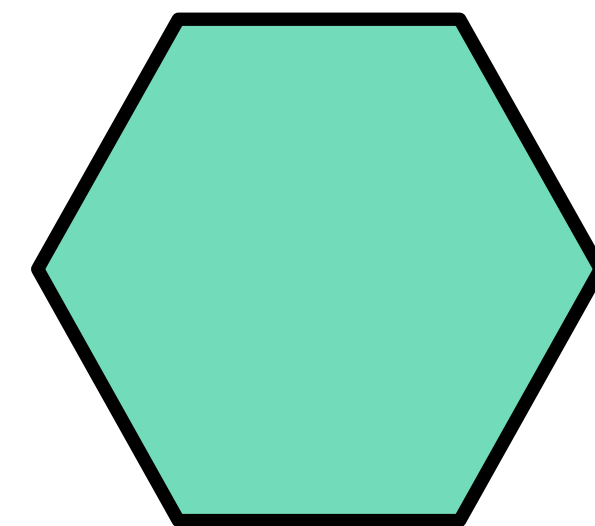
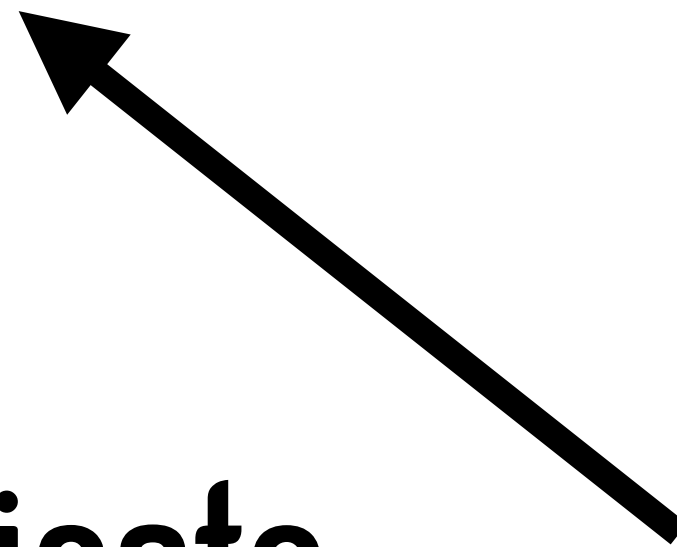
**Your servers.**



**Certificate authority.**



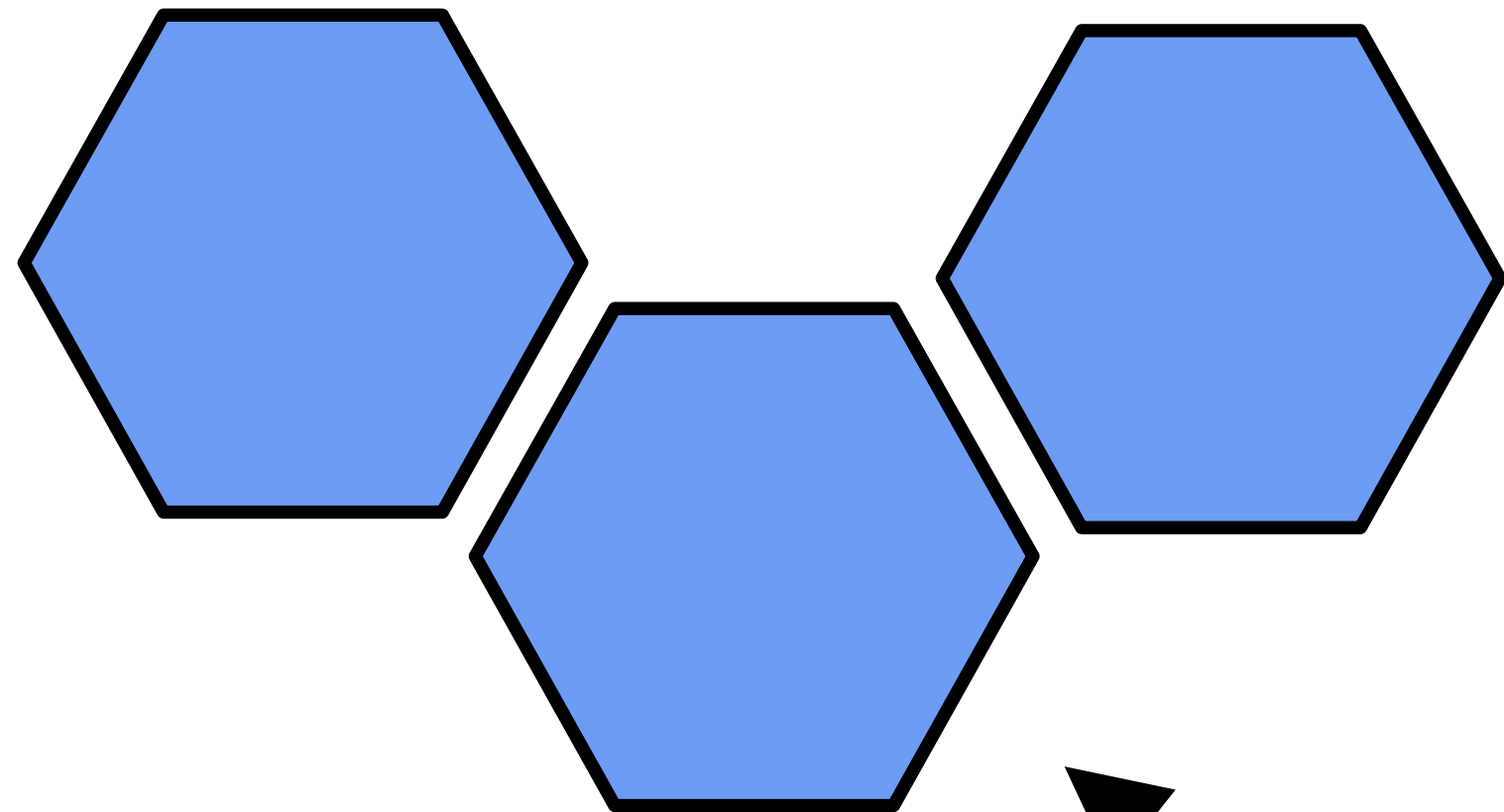
**Servers log certificate attributes.**



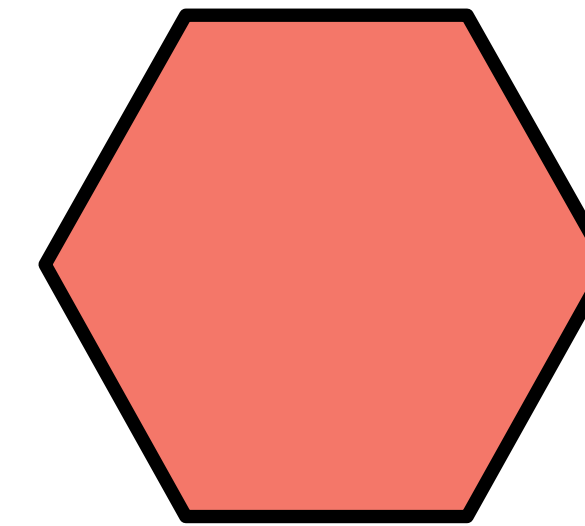
**You.**



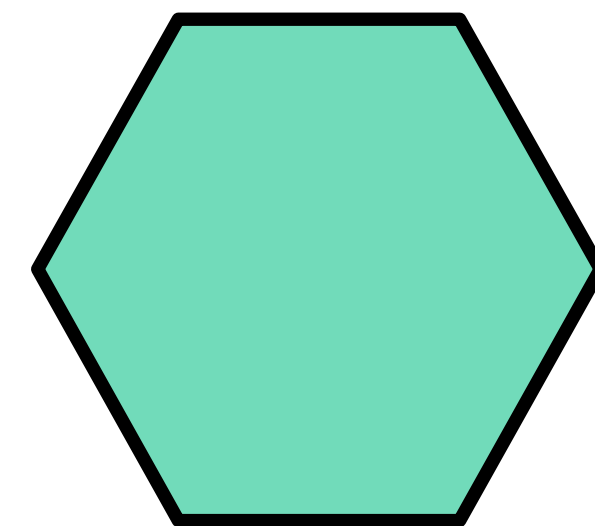
**Your servers.**



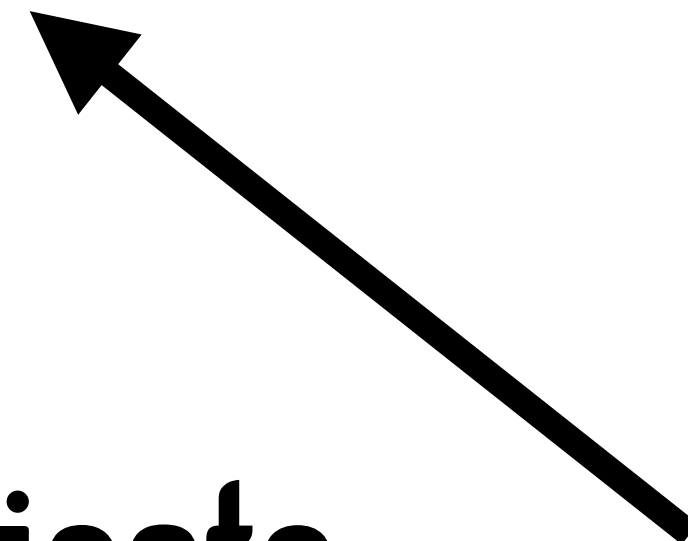
**Certificate authority.**



**Servers log certificate attributes.**



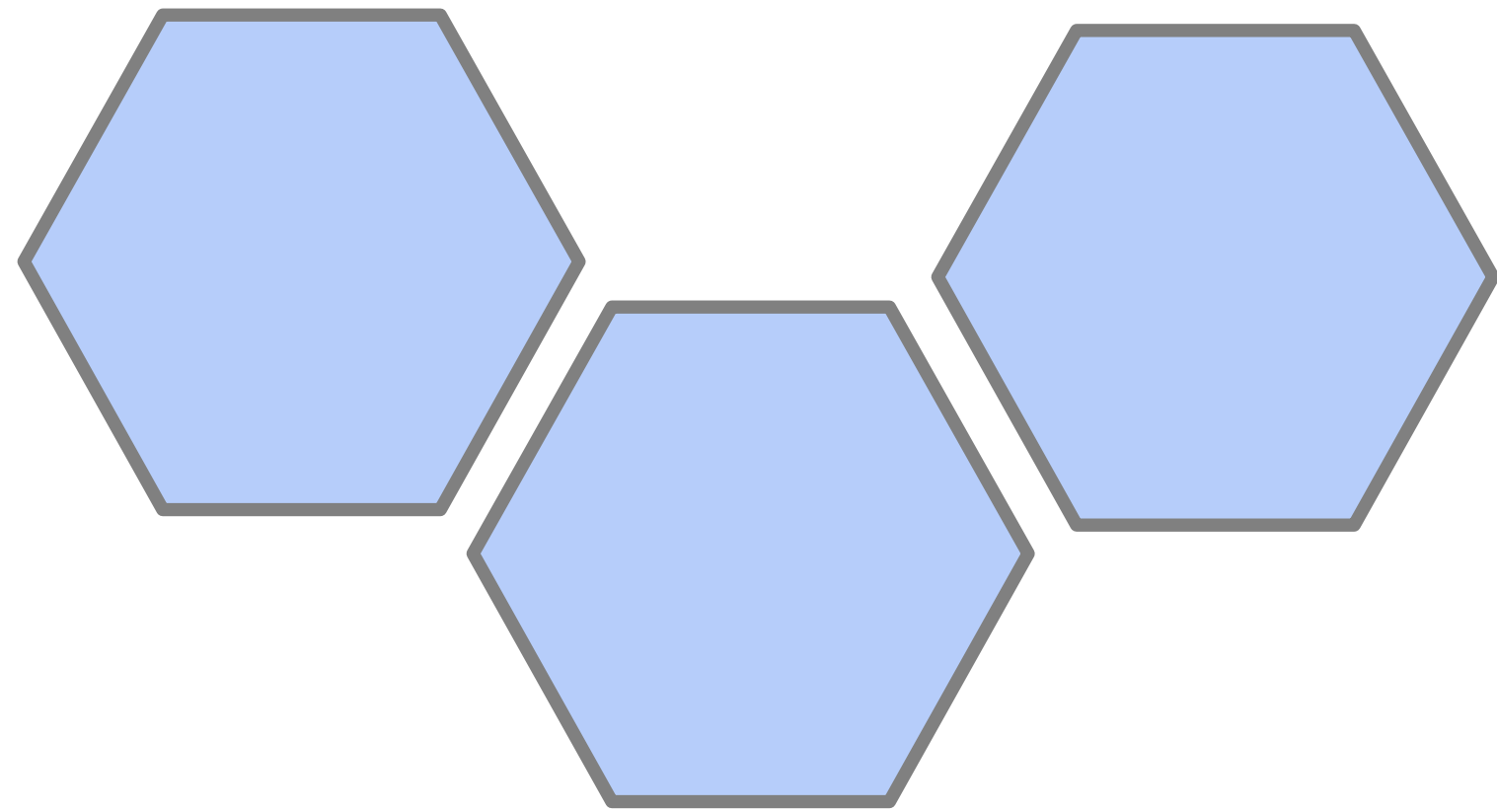
**You.**



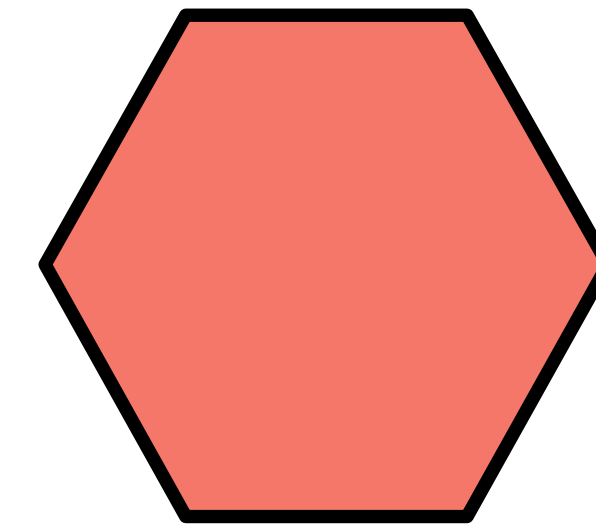
**This means the authorities audit records can be matched against actual access to verify behaviours.**



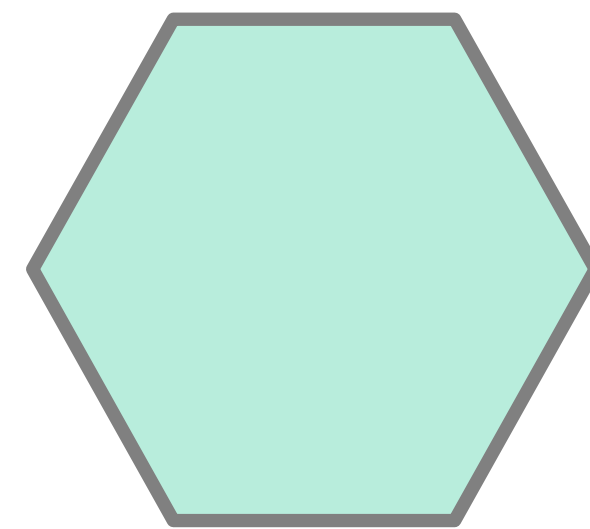
Your servers.



Certificate authority.



**Users and access can be managed at certificate authority.**

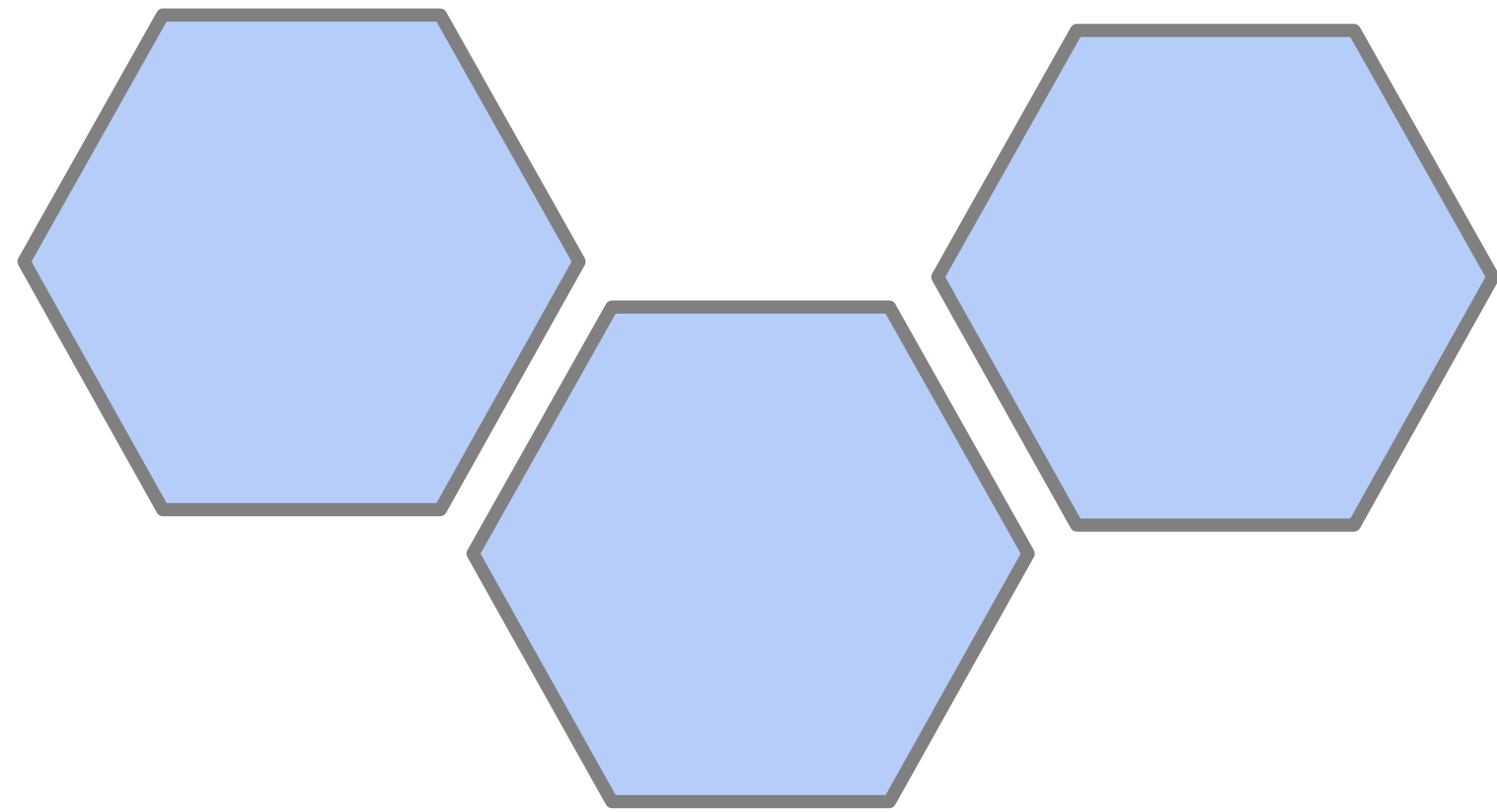


You.

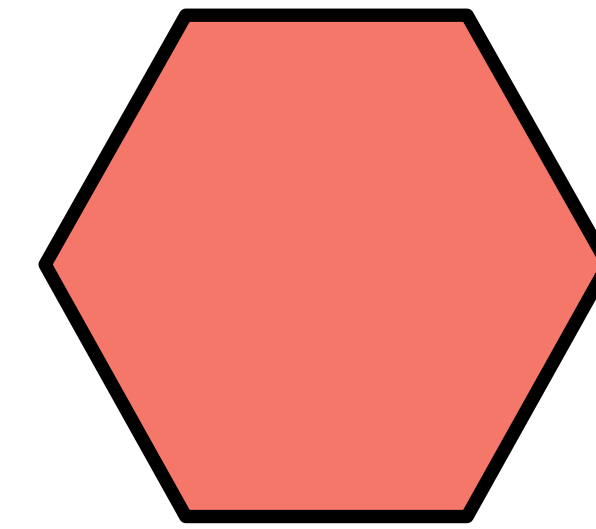




Your servers.



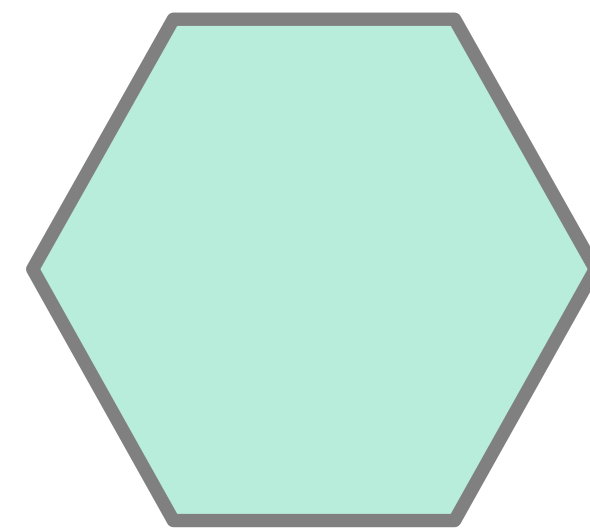
Certificate authority.



Users and access can be managed at certificate authority.



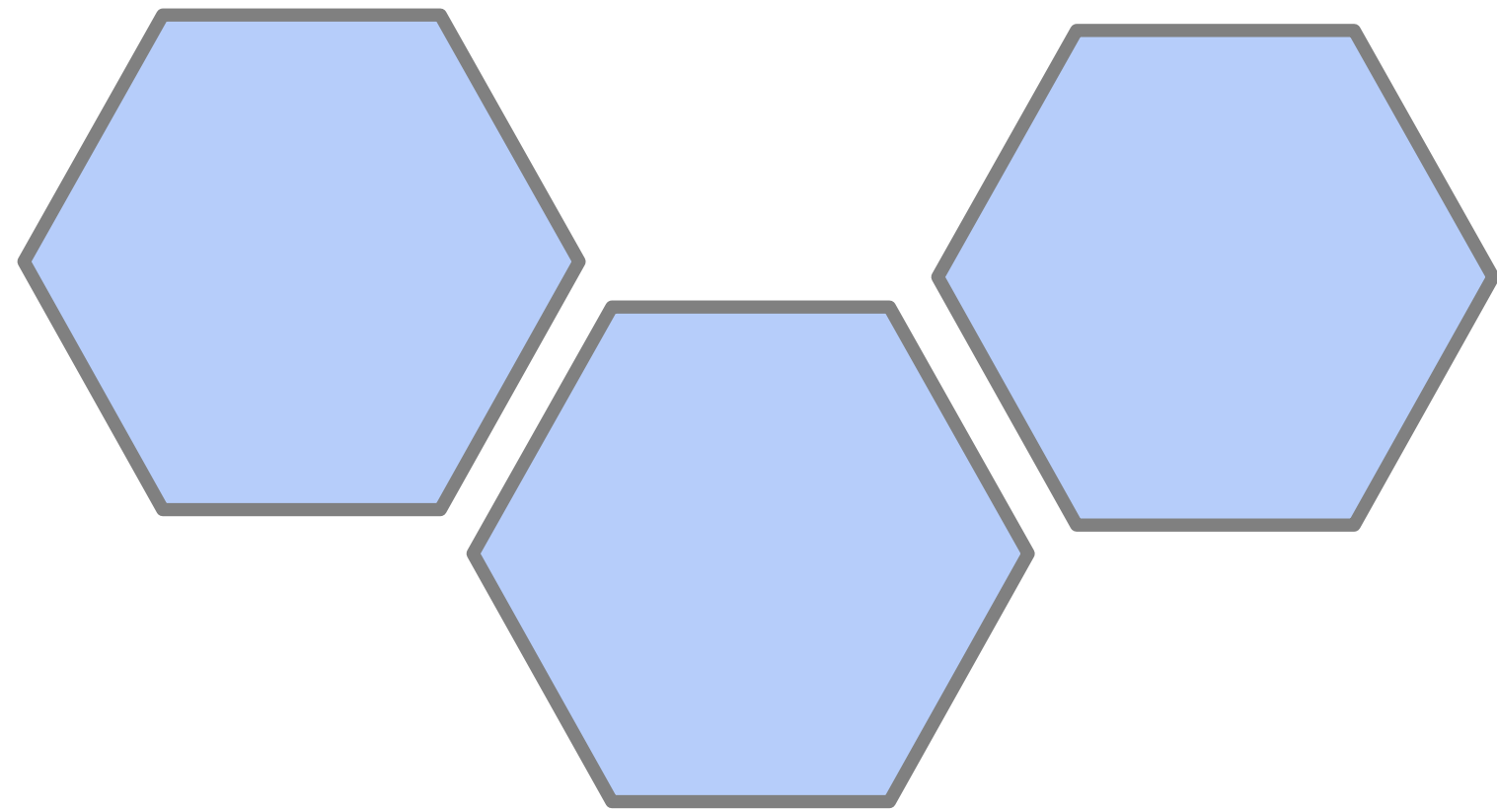
This means we don't have to reconfigure servers or resort to fragile always-on centralised systems to revoke access.



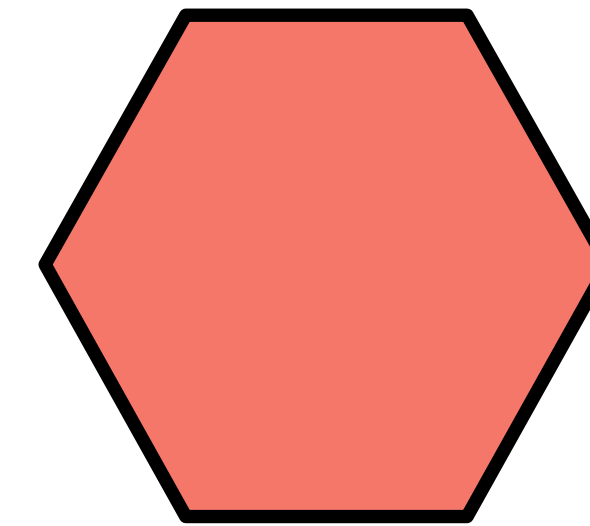
You.



Your servers.



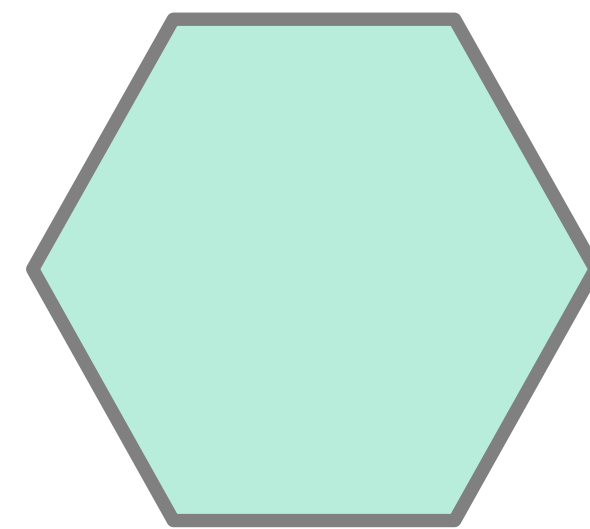
Certificate authority.



Users and access can be managed at certificate authority.



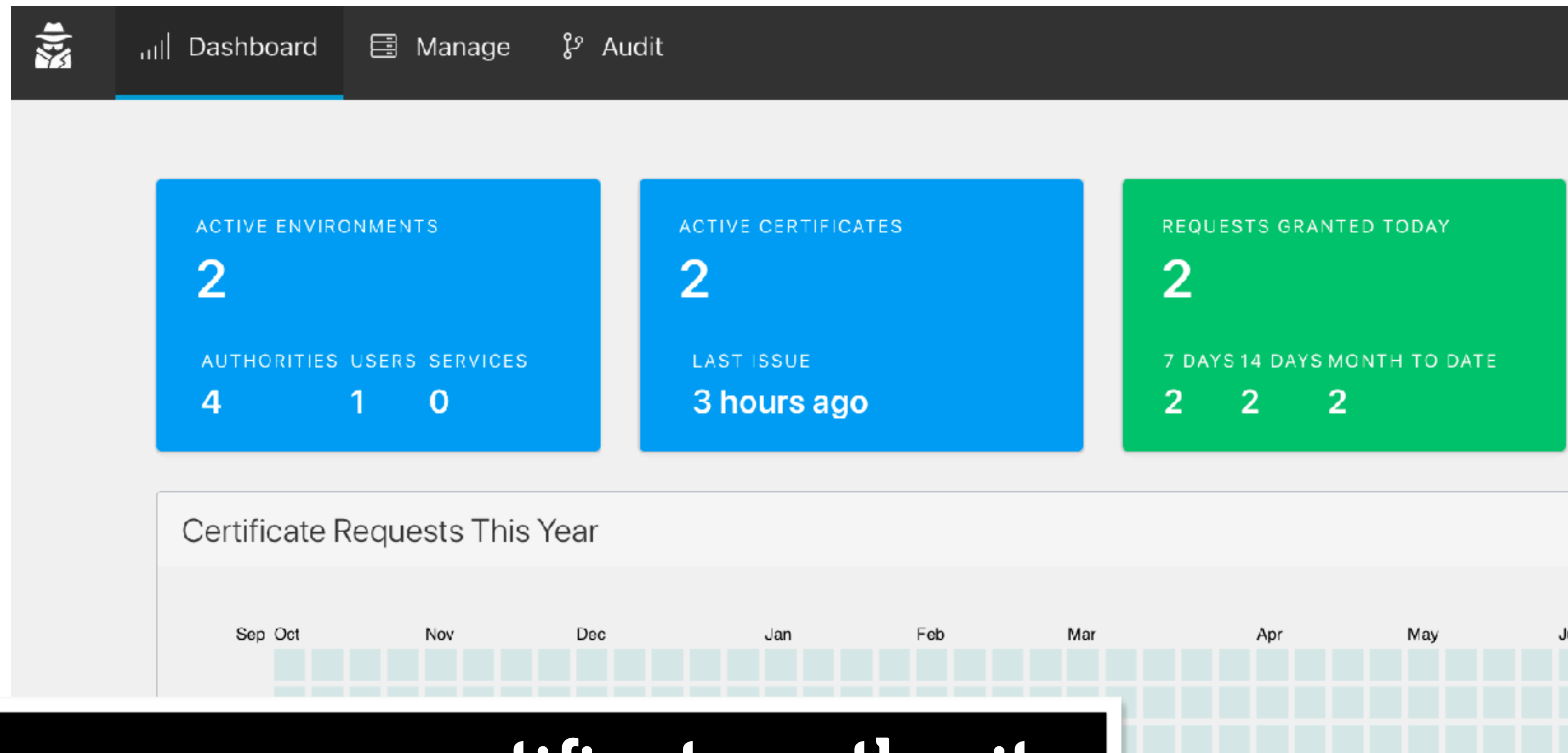
This means off-boarding users is a single action, no complex update, no forgotten keys.



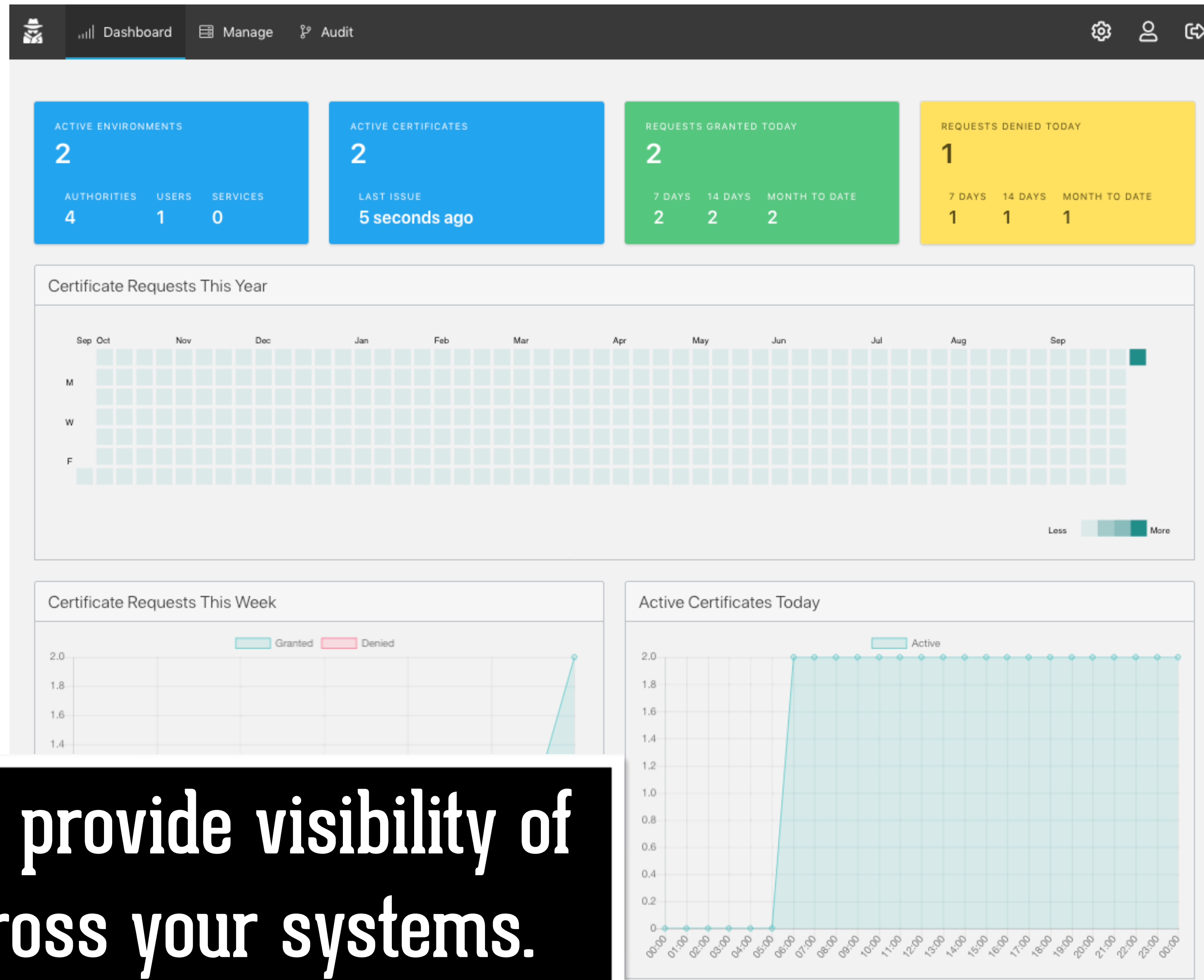
You.

**How does Smith help?**





**Smith manages your certificate authority, verifying access and performing contextual checks.**



**Dashboards provide visibility of access across your systems.**



Dashboard Manage Audit

Manage [Add Environment](#)

### simpsons

ACTIVE CERTIFICATES  
**0**  
LAST ISSUE  
No active certificates

CERTIFICATE REQUESTS THIS YEAR

	Se	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
M													
W													
F													

Less More

[Manage](#)

### muppets

ACTIVE CERTIFICATES  
**2**  
LAST ISSUE  
3 minutes ago

CERTIFICATE REQUESTS THIS YEAR

	Se	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
M													
W													
F													

Less More

[Manage](#)

Manage as many environments  
as you need.



Dashboard Manage Audit

2018-09-23T06:43:46Z  
Username: lumbergh  
Host: smith-demo-host  
Principals: root  
Environment: muppets  
Certificate Authority: ca-0  
**Certificate issued for duration: 1 day**

2018-09-23T06:43:46Z  
Username: lumbergh  
Host: smith-demo-host  
Principals: root  
Environment: muppets  
Certificate Authority: ca-0  
**Certificate issued for duration: 1 day**

2018-09-23T06:43:46Z  
Username: lumbergh  
Host: smith-demo-host  
Principals: root  
Environment: simpsons  
Certificate Authority: ca-0  
**Access denied.**

Detailed audit trail of all access.



Dashboard Manage Audit

## Administration

TEAM SETTINGS

- User Accounts
- Service Accounts
- Teams**
- Roles

ORGANISATION SETTINGS

- Authentication
- Billing

Teams	Name
	engineering
	operations

+

**Flexible, easy to manage users,  
teams, roles and permissions.**





```
2. mth@space: ~ (docker)
darth $ smith
Usage: smith ((-v|--version) | COMMAND)

Available options:
  -v, --version      Version information
  -h, --help         Show this help text

Available commands:
  issue              Request a certificate and configure ssh-agent.
  connect            Request a certificate, configure ssh-agent, run
                    provided command.
  userinfo           Request userinfo for authenticated identity.
  provision          Get CA public keys.
darth $ smith connect -- ssh user@server
```

**Command line tools that integrate  
with current workflows.**

Overall Smith improves the tools you have for access control. Smith makes things **easier** for operations, **easier** for users and more **secure** for everyone.





**smith**  
secure access made easy

contact us: [mark@smith.st](mailto:mark@smith.st) or [navin@smith.st](mailto:navin@smith.st)