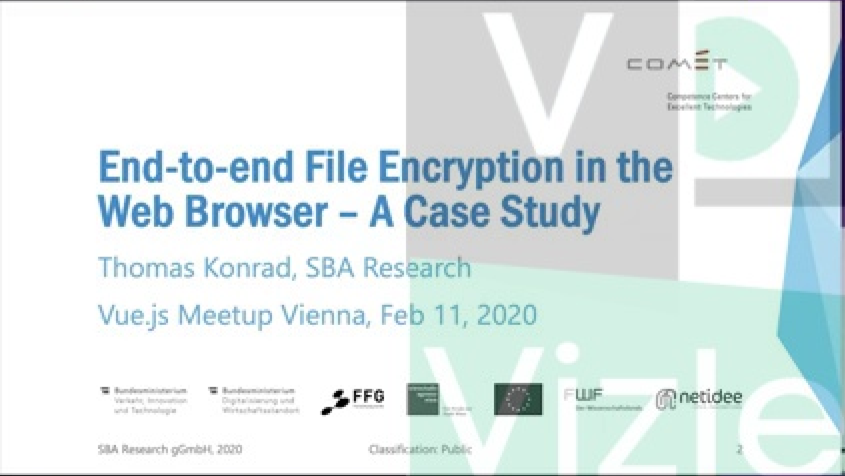
Talk presented at

Vue.js Vienna

Video recorded by PUSHER



COMET

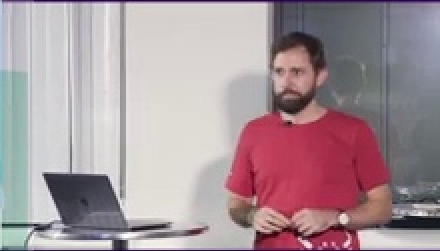
Competence Centers for Excellent Technologies

# End-to-end File Encryption in the Web Browser – A Case Study

Thomas Konrad, SBA Research

Vue.js Meetup Vienna, Feb 11, 2020

Bundesministerium Verkehr, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG
FWF
netidee



Talk presented at

Vue.js Vienna

Video recorded by

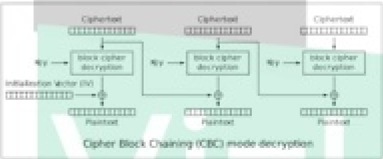
PUSHER

# Ensure Confidentiality, Integrity, and Authenticity

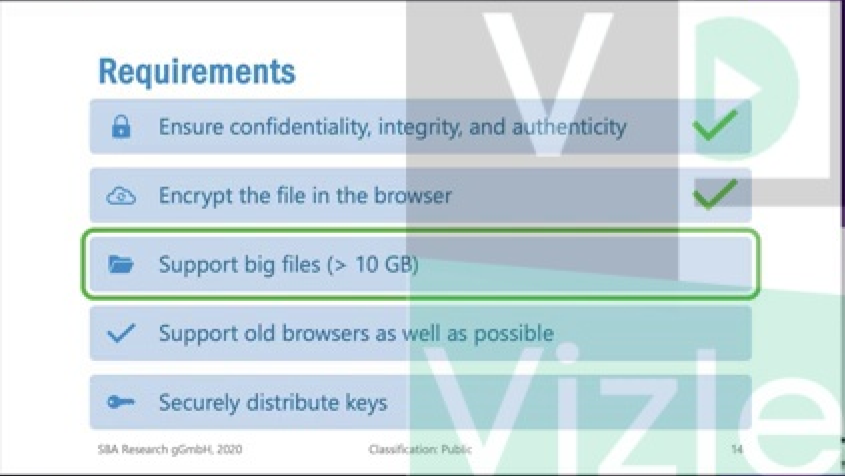
Let’s take as an example **AES** in **CBC** mode.

What do you think we can guarantee with it?

- ✓ **Confidentiality**
- **Integrity**
- **Authenticity**



Cipher Block Chaining (CBC) mode decryption

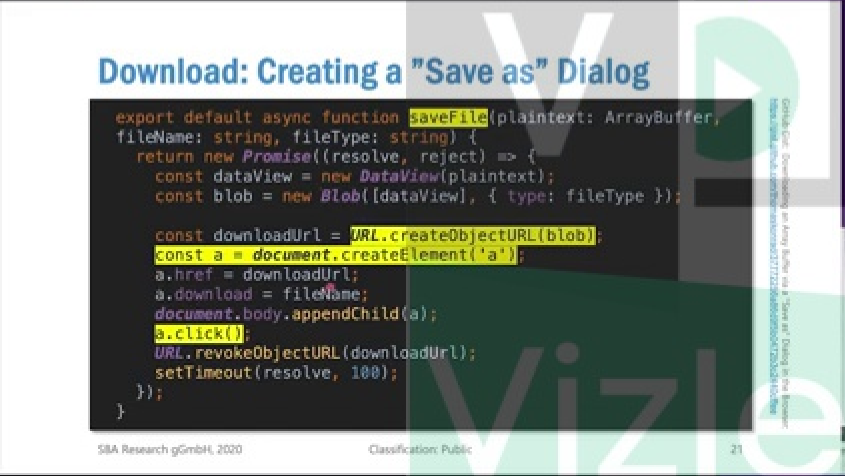


## Requirements

- 🔒 Ensure confidentiality, integrity, and authenticity ✓
- Encrypt the file in the browser ✓
- Support big files (> 10 GB)
- ✓ Support old browsers as well as possible
- Securely distribute keys

Talk presented at
Vue.js Vienna

Video recorded by
PUSHER



## Download: Creating a "Save as" Dialog

```
export default async function saveFile(plaintext: ArrayBuffer,
fileName: string, fileType: string) {
  return new Promise((resolve, reject) => {
    const dataView = new DataView(plaintext);
    const blob = new Blob([dataView], { type: fileType });

    const downloadUrl = URL.createObjectURL(blob);
    const a = document.createElement('a');
    a.href = downloadUrl;
    a.download = fileName;
    document.body.appendChild(a);
    a.click();
    URL.revokeObjectURL(downloadUrl);
    setTimeout(resolve, 100);
  });
}
```

GitHub Gist: Downloading an Array Buffer via a "Save as" Dialog in the Browser: [illegible]

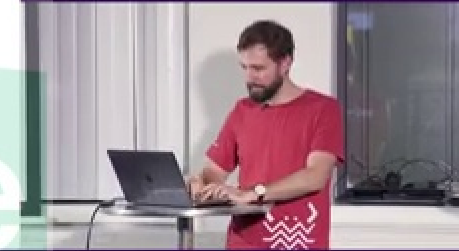
SBA Research gGmbH, 2020 Classification: Public 21

Talk presented at

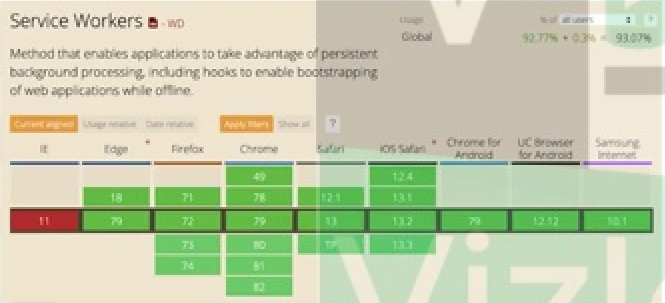
Vue.js Vienna

Video recorded by

PUSHER



# Service Workers: Browser Support



## Service Workers - WD

Usage: Global 92.77% + 0.3% = 93.07%

Method that enables applications to take advantage of persistent background processing, including hooks to enable bootstrapping of web applications while offline.

| IE | Edge * | Firefox | Chrome | Safari | iOS Safari * | Chrome for Android | UC Browser for Android | Samsung Internet |
|---|---|---|---|---|---|---|---|---|
| | | | 49 | | 12.4 | | | |
| | 18 | 71 | 78 | 12.1 | 13.1 | | | |
| 11 | 79 | 72 | 79 | 13 | 13.2 | 79 | 12.12 | 10.1 |
| | | 73 | 80 | TP | 13.3 | | | |
| | | 74 | 81 | | | | | |
| | | | 82 | | | | | |

Talk presented at
Vue.js Vienna

Video recorded by
PUSHER

build: build 2.6.0-beta.2
test: dynamic directive arguments for v-on, v-bind and custom directives
perf: improve scoped slots change detection accuracy
test: test cases for v-on/v-bind dynamic arguments
refactor: v-bind dynamic arguments use bind helper
test: handle dynamic arguments for v-bind.sync
origin/slot-optimization
test: dynamic directive arguments for v-bind and v-on
fix: fix checkbox event edge case
test: fix tests in IE/Edge

# Demo Time!

SBA Research gGmbH, 2020

Photo by Yancy Min on Unsplash

Talk presented at
Vue.js Vienna

Video recorded by
PUSHER