AWS CloudFormation and CDK doesn't support AWS SSM Parameter Store SecureString?!

Date:	2024-05-12
modified:	2024-07-17
tags:	AWS, SSM, CloudFormation, CDK, Lambda
description:	AWS SSM Parameter Store SecureString type not usable with CloudFormation and AWS CDK
category:	Cloud
slug:	aws-cloudformation-and-cdk-doesnt-support-aws-ssm-parameter-store-securestring
Author:	Dominik Wombacher
lang:	en
transid:	aws-cloudformation-and-cdk-doesnt-support-aws-ssm-parameter-store-securestring
Status:	published

I recently started to set up some resources on AWS for my side projects. For starters an AWS KMS key so I can encrypt data on S3 and in the AWS SSM Parameter Store. To use S3 and DynamoDB as backend and perform end-to-end state encryption for OpenTofu, I also needed an IAM User. So the Idea was to write a CloudFormation template that creates all these resources for me and then use it to deploy other Infrastructure as code via OpenTofu. I'm not a huge fan of IAM Users and access keys, but in this case good enough to get started.

What I wanted: The generated access and secret key are stored in AWS SSM Parameter store. That way I don't have to deal with clear text credentials in CloudFormation.

SSM Parameter Store can save Strings and SecureStrings. As the name implies, a SecureString is encrypted via AWS KMS before put into SSM Parameter Store. But then I learned, neither Cfn nor CDK support it. They can only write clear text Strings to the Parameter Store. What a bummer and pretty unexpected.

So after some research, a Cfn CustomResource is what I need. It's basically a Lambda function that receives a Create/Update/Delete request from Cfn, performs an action and sends the result back to the Stack. It took me a bit to get something together but now it works like a charm.

I'm still a bit disappointed that such a common feature isn't supported. Arguments are mostly that Cfn and CDK are not supposed to deal with secrets. I can understand that, but putting some data that were generated during a Cfn run into the parameter store can't be that unique.

I published my Lambda Function to interact with AWS SSM Parameter Store SecureString under MIT: https://git.sr.ht/~wombelix/cfn-custom-resource-aws-ssm-securestring